MAANPUOLUSTUSKORKEAKOULU

WLAN TAISTELUKENTÄLLÄ

Tutkielma

Kapteeni
Mikko Rasimus

EUK 66
Maasotalinja

Huhtikuu 2014

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
Esiupseerikurssi 66	**Maasotalinja**
Tekijä **Kapteeni Mikko Rasimus**	
Tutkielman nimi **WLAN TAISTELUKENTÄLLÄ**	
Oppiaine johon työ liittyy Sotatekniikka	Säilytyspaikka MPKK:n kurssikirjasto
Aika Huhtikuu 2014	Tekstisivuja 38 Liitesivuja 16

TIIVISTELMÄ

Taistelukentällä tapahtuva johtaminen on muuttunut 2010-luvulle tultaessa informaatioajan johtamiseksi, jossa käytettävissä olevan informaation määrä on kasvanut huomattavasti perinteisiin sotiin verrattuna. Antiikin taisteluissa joukon komentaja näki koko taistelukentän ja kykeni luomaan ymmärryksen tilanteesta silmien edessä aukeavan kuvan perusteella. Nykyisin komentajalle luodaan tiedustelun tuottama kuva vihollisen toiminnasta, omien joukkojen välittämä kuva omasta ryhmityksestä sekä esikuntien rakentama malli siitä, kuinka tilannekuvan osat liittyvät suunniteltuun kokonaisuuteen. Taistelukentällä joudutaan toimimaan olosuhteissa, joissa ei ole mahdollisuutta kytkeytyä laajakaistaiseen tiedonsiirtoverkkoon – lähiverkkoon eikä runko- tai liityntäverkon viestiasemaan.

Tutkimus on lähtökohdiltaan kvantitatiivinen tapaustutkimus. Käytettävinä tutkimusmenetelminä ovat kirjallisuustutkimus, vaatimusmäärittely ja kenttäkokeet. Tutkimuksessa määritellään toiminnalliset ja tekniset vaatimukset WLAN-standardien mukaisille verkoille ja laitteille kolmessa rajatussa tapauksessa. Kenttäkokeilla on selvitetty tekniset ratkaisut ja asetukset, joilla tapaukset voidaan toteuttaa. Johtopäätökset on tehty hypoteettis – deduktiivisella päättelyllä. Tutkimustulosten yleisempää käytettävyyttä ajatellen tutkituista kokonaisuuksista on pyritty tekemään johtopäätöksiä myös tutkimustapauksista poikkeavissa olosuhteissa.

Tutkimuksen perusteella tiedonsiirtojärjestelmän tulee jatkuvasti kyetä välittämään tilannetiedot riittävän tilannekuvan muodostamiseksi luotettavasti, eheänä ja oikea-aikaisesti. Verkkojen tulee mahdollistaa käyttäjän pääsy hänelle kuuluvaan tietoon. Verkon tiedonsiirtokapasiteetin tulee olla riittävä. Päätelaitteiden tulee kyetä liittymään eri verkkoihin viiveettömästi ilman asetusten muuttamista. Parhaiten näihin vaatimuksiin vastaavat Linux-pohjaiset solmut, jotka tukevat uusinta standardia.

Rakennettaessa langatonta verkkoa rajattuun käyttöympäristöön tulee järjestelmään hankittavat laitteet kokeilla suunnitelluilla asetuksilla, jotta voidaan varmistua laitteiden ja asetusten toimivuudesta halutulla tavalla.

AVAINSANAT

WLAN, lähiverkko, langaton lähiverkko, AdHoc, Access Point

Sisältö

Kuvat

Lyhenteet

AP	Access Point (Tukiasema)
AdHoc	Langattoman lähiverkon arkkitehtuuri, jossa ei käytetä tukiasemaa
BSS	Basic System Set, topologialtaan yksinkertainen langaton verkko
ESS	Extended Service Set, erillisistä BSS-verkoista muodostettu verkko
IBSS	Independent BSS, ks. AdHoc
IP	Internet Protocol
GAN	Global Area Network (Globaaliverkko)
LAN	Local Area Network (Lähiverkko)
MAC	Media Access Control
MAN	Metropolitan Area Network (Alueverkko)
MICS	Multi Interface Communication Software
MIMO	Multiple Input Multiple Output, langattoman lähiverkon tekniikka, jossa käytetään useampaa, kuin yhtä antennia
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network (Etäverkko)
WDS	Wireless Distribution System
WLAN	Wireless Local Area Network (Langaton lähiverkko)

WLAN TAISTELUKENTÄLLÄ

1. JOHDANTO

Taistelukentällä tapahtuva johtaminen on muuttunut 2010-luvulle tultaessa informaatioajan johtamiseksi. Siinä korostuvat pyrkimys reaaliaikaiseen tilannekuvaan ja tiedonsiirtoverkoissa välitettävän datan kasvanut määrä. Muutoksen voidaan katsoa käynnistyneen 1990-luvulla. Muutokseen on johtanut moni toisistaan riippumaton seikka. Kylmän sodan jälkeen tapahtunut muutos massamaisista joukoista pienempiin ja entistä teknisempiin joukkoihin on vaikuttanut osaltaan tarpeeseen kehittää joukkojen suorituskykyjä teknisillä välineillä [15, s. 18].

Tietotekniikan kehittyminen ja henkilökohtaisten tietokoneiden (PC) lisääntyminen helpottivat kirjallisen materiaalin tuottamista ja käsittelyä. Tietojen siirtäminen tietokoneelta toiselle oli kuitenkin hankalaa ja syntyi tarve koneiden yhdistämiselle, verkottamiselle. Internetin siirtyminen operaattoreiden haltuun ja siitä alkanut leviäminen 1990-luvun puolenvälin jälkeen osoitti tietoverkkojen mukanaan tuomia mahdollisuuksia ja sotilaallisissa yhteyksissä alettiin kehittää taistelukentällä toimivaa integroitua tiedonsiirtoverkkoa – ”taktista internetiä”.

Tietokoneiden teknisen verkottamisen myötä kehitettiin erilaisia verkostokeskeisen ja myöhemmin vaikutusperustaisen sodankäynnin teorioita. Verkostokeskeisen sodankäynnin teoria korosti aluksi teknisiä hyötyjä ja tehokkaiden tiedonsiirtoyhteyksien muodostamaa verkostoa. Teorian kehittyessä painopiste siirtyi johtamiseen ja suunnitteluun. Verkottumisen rooli muodostui sodankäyntiä tukevaksi ja johtamisen sekä suunnittelun tarpeet asettivat vaatimukset johtamisjärjestelmille.[15]

Johtamisen ja suunnittelun tarpeet reaaliaikaiselle tilannekuvalle asettavat vaatimuksia johtamisjärjestelmien tiedonsiirtokapasiteetille. Perinteisten analogisten radio- ja puhelinyhteyksien tiedonsiirtokapasiteetti on rajattu. Laajakaistaiset pakettikytkentäiset verkot mahdollistavat huomattavasti suuremman tiedonsiirtokapasiteetin. Johtamis- ja komentopaikkojen sisäiset yhteydet on helppo toteuttaa nykyisillä lähiverkkotekniikoilla. Kehittynyt linkkitekniikka mahdollistaa laajakaistaisen tiedonsiirron myös taistelukentän runko- ja liityntäverkoissa. Johtamispaikat ja liittyjät saadaan siis liitettyä johtamisverkkoon yhteyksillä, joilla on riittävä tiedonsiirtokapasiteetti.

Johtajan osuus on tilannekuvan luomisessa oleellinen. Teknisesti voidaan katsoa johtajan hallussa olevan päätelaitteen olevan vielä johtajaakin kriittisempi tekijä tapauksissa, jossa päätelaite, kuten MATITSTJJ-pääte välittää sijaintitietonsa verkkoon automaattisesti. Johtaja joutuu toimimaan olosuhteissa, joissa ei ole mahdollisuutta kytkeytyä laajakaistaiseen tiedonsiirtoverkkoon – lähiverkkoon eikä runko- tai liityntäverkon viestiasemaan. Tässä tutkimuksessa tutkitaan kolmea rajattua tapausta, joissa johtaja pyrkii liittämään päätelaitteensa edellä mainittuihin verkkoihin langattoman lähiverkon (WLAN) välityksellä.

1.1. Aiemmat tutkimukset

Taistelukenttää ja taistelukentän muutoksia on tutkittu paljon. Aiheesta löytyy useita sekä kotimaisia että ulkomaisia julkaisuja. Julkaisut ja tutkimukset ovat omalla tavallaan aikansa kuvauksia. Kotimaisesta lähdeaineistosta mainittaviksi nousevat Maanpuolustuskorkeakoulun taktiikan laitoksen julkaisut, joissa on julkaistu laitoksella tehtyjä tutkimuksia, opettajien artikkeleja sekä erilaisten seminaariesitysten pohjalta kirjoitettuja artikkeleja. Tutkimukset ja artikkelit pohjautuvat toimintaympäristössä tapahtuneisiin muutoksiin, havaintoihin viime vuosikymmenien sotakentiltä sekä osittain kirjoittajien näkemyksiin ja arvioihin tulevaisuuden toimintaympäristöstä.

Tämän työn kannalta Maanpuolustuskorkeakoulun Taktiikan laitoksen taistelutilaa koskevista tutkimuksista on lähteinä käytetty Mika Huttusen *Monimutkainen taktiikka* ja Teemu Nurmelan *Sotilaallisen kriisinhallintajoukon taistelutilaan vaikuttavat tekijät.* Huttusen teos on julkaistu vuonna 2010. Teos käsittelee taktiikan käsitteitä laajemminkin ja perustuu kattavasti kotimaisiin ja ulkomaisiin lähteisiin. Taistelutilan määrittelyssä Huttunen on käyttänyt yhdysvaltalaisia määritteitä ja Michael Keanen sanakirjaa *Dictionary of Modern Strategy and Tactics*, jota on käytetty tämänkin tutkimuksen lähteenä. Nurmelan tutkimus keskittyy kriisinhallintaympäristöön ja lähteinä on käytetty runsaasti YK:n ja Yhdysvaltain armeijan normeja. Nurmela on viitannut Huttusen vuonna 2005 julkaistuun *Näkökulmia taktiikkaan – Taktiikan käsite ja taktiikan keinot tulkinnan kohteena* sekä kirjoitushetkellä luonnoksena olleeseen *Yhtymän suunnitteluperusteet* julkaisuun. Yhtymän suunnitteluperusteet on julkaistu vuonna 2010 nimellä *Maavoimien yhtymän suunnittelun ja päätöksenteon perusteet*, jonka määritelmään on viitattu tässä tutkimuksessa.

Kansainväliset tutkimukset sekä sotakokemuksiin perustuvat kirjoitukset eivät ole suoraan rinnastettavissa Suomeen, koska toimintaympäristöt ja tutkittavat joukot ja ilmiöt ovat osin erilaisia. Toisaalta myös vahvasti tulevaisuutta visioivat kirjoitukset vaativat kriittistä tarkastelua pohdintojen perusteista ja johtopäätöksiin johtaneista seikoista. Lähteenä käytetyt kirjoitukset muodostavat kuitenkin kokonaisuuden ja niistä saa hahmotettua kuvan taistelukentällä tapahtuneesta muutoksesta ja muutoksen aiheuttamista vaatimuksista tämän päivän ja osin tulevaisuudenkin johtamisjärjestelmille. Yhdysvaltain varapuolustusministerin alainen tutkimusohjelma The Command and Control Research Program within the Office of the Assistant Secretary of Defence (CCRP) julkaisee useita aiheeseen liittyviä tutkimuksia vuosittain. Tutkimusten luotettavuutta voidaan pitää hyvänä ja globaaleja ilmiöitä kuvaavia tutkimustuloksia voidaan hyödyntää sellaisenaan. Tässä tutkimuksessa CCRP:n julkaisuista on lähteenä käytetty Albertsin ja Hayesin tutkimuksia johtamisesta ja suunnittelusta.

Lähiverkkoja, niiden tekniikkaa ja langattomia sovelluksia on tutkittu paljon Suomessa ja maailmalla. Tarkasti standardoitu tekniikka ja suuri määrä tutkittua tietoa antavat varmuuden teknisten yksityiskohtien oikeellisuudesta ja lähdemateriaalin reliabiliteetista. Myös langattoman lähiverkon soveltuvuutta erilaisiin tarkoituksiin ja ympäristöihin on tutkittu runsaasti. Maanpuolustuskorkeakoululla on tehty opinnäytetöitä langattoman lähiverkon soveltuvuudesta erilaisiin sotilaallisiin sovelluksiin. Juha Peltomäki on tutkinut diplomityössään kenttätelelääkinnän toteuttamisratkaisua ja esitellyt työssään lyhyesti langatonta tiedonsiirtoa, sen standardeja ja tekniikoita. Jussi Timonen on diplomityössään *A Dynamic Tactical Command System Operating with an Ad Hoc Network* Turun yliopiston Informaatiotekniikan laitoksella käsitellyt AdHoc-verkkojen käytettävyyttä sotilaallisessa ympäristössä. Työssä on kuvailtu aiempaa aiheesta tehtyä tutkimusta sekä tutkittu johtamiseen ja joukkojen siirtoon käytettävää järjestelmää AdHoc-verkossa demoympäristössä. Työn painopiste on järjestelmän tutkimisessa, käytettävyydessä sekä käyttäjäkohtaisissa näkymissä. Työssä on esitetty vaatimuksia järjestelmälle, laitteille ja sovellukselle.

Tämän tutkimuksen kannalta merkittävä lähde on myös Jarkko Karsikkaan diplomityö *Maavoimien verkostokeskeisen tiedonsiirtojärjestelmän arkkitehtuuri ja sen toteuttaminen*. Karsikas tutkii työssään työn otsikon mukaisesti Maavoimien tiedonsiirtojärjestelmän arkkitehtuuria. Tutkimuksen aihe luo osaltaan viitekehyksen tälle tutkimukselle. Tämän tutkimuksen tapaukset kuvaavat pienen osan Maavoimien tiedonsiirtojärjestelmästä. Karsikas kuvaa diplomityössään ansiokkaasti toimintaympäristössä tapahtunutta muutosta ja tiedonsiirtojärjestelmälle asetettavia vaatimuksia keskittyen lähinnä Suomeen ja Yhdysvaltoihin.

1.2. Tutkimusongelma ja tutkimuksen rakenne

Tämän tutkimuksen päätutkimusongelma on:

- Voidaanko WLAN-perustaisia järjestelmiä käyttää tiedonsiirtoon taistelukentän/taistelutilan olosuhteissa?

Päätutkimusongelmaan on pyritty vastaamaan ratkaisemalla seuraavat alakysymykset:

- Mitkä ovat toiminnalliset vaatimukset (taistelevan joukon operatiiviset/taktiset vaatimukset) WLAN-perustaiselle tiedonsiirtojärjestelmälle?
- Mitkä ovat tekniset vaatimukset WLAN-perustaiselle tiedonsiirtojärjestelmälle?

Tutkimuksen johdannossa esitellään lyhyesti tutkimuksen tausta ja toimintaympäristön muutoksen aiheuttama tarve tutkimukselle. Tutkimuksen rajaukset ja viitekehys sekä tutkimuksen rakenne ja tutkimusmetodologia esitellään johdannon lopussa.

Tutkimuksen toisessa ja kolmannessa luvussa kuvataan taistelukenttä toimintaympäristönä, suunnittelun ja johtamisen vaatimukset johtamisjärjestelmälle sekä WLAN tiedonsiirtotekniikkana. Luvuissa määritellään perusteet alatutkimuskysymyksille.

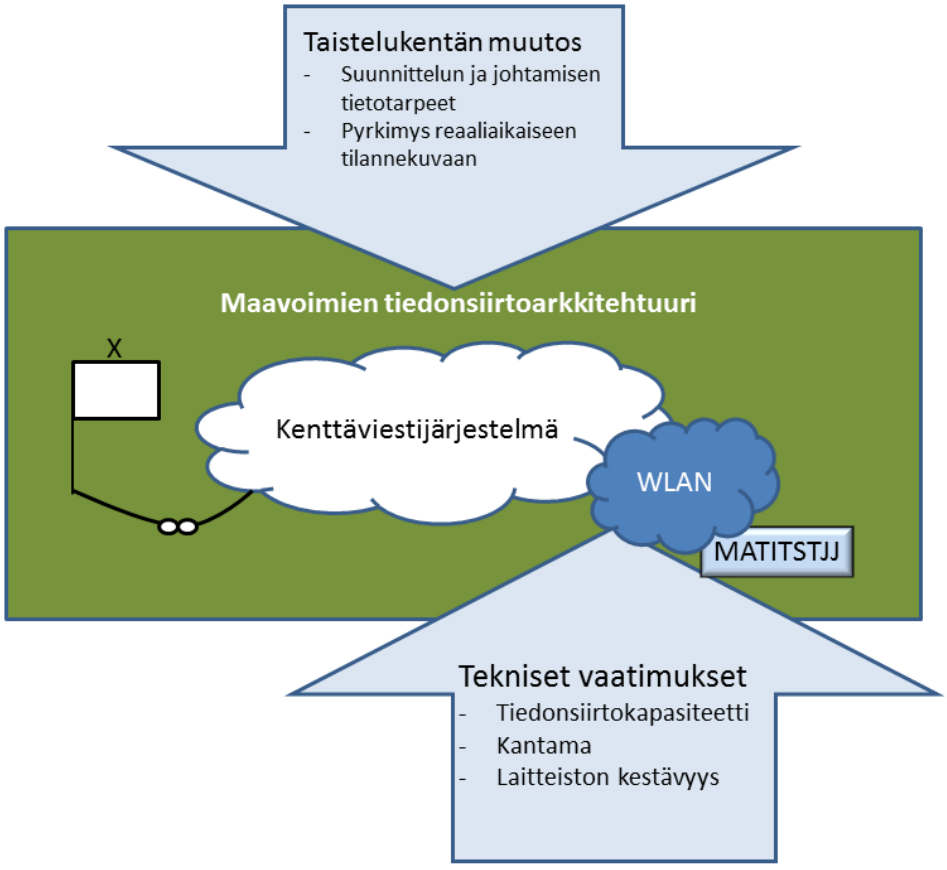
Luvussa neljä esitetään tutkimuksen tapausten olosuhteet ja tekniset ratkaisut sekä toteutus. Luvussa tehdään johtopäätökset tutkittavista tapauksista ja esitetään tutkimustapausten erityispiirteet tutkimuksen pääongelman näkökulmasta. Tutkimuksen yhdistelmäluvussa vastataan tutkimuksen pääongelmaan. Lukujen kaksi, kolme ja neljä perusteella luodut vaatimukset kootaan johtopäätösluvussa vastauksiksi alatutkimuskysymyksiin.

Ensimmäisessä alatutkimuskysymyksessä selvitetään toiminnallisia vaatimuksia taktisen ja operatiivisen tason näkökulmasta. Taisteluteknisen tason, ryhmä – komppania, vaatimukset käsitetään tässä tutkimuksessa teknisinä vaatimuksina. Esimerkiksi joukon ryhmitys on taistelutekninen suorite, joka luo teknisen vaatimuksen langattomalle lähiverkolle yhteysetäisyyden vähimmäismittana.

1.3. Rajaukset ja tutkimuksen viitekehys

Tässä tutkimuksessa tutkitaan langattoman lähiverkon (WLAN) käytettävyyttä taistelukentän olosuhteissa. Tutkimus on rajattu kolmeen tapaukseen, joissa jokaisessa tutkitaan päätelaitteen liittämistä langattomaan lähiverkkoon. Tapausten toimintaympäristöt ja tekniset ratkaisut poikkeavat toisistaan. Liitettävä päätelaite on sama, mutta tukiasemien / reitittimien ratkaisut poikkeavat toisistaan. Tutkimus on rajattu käsittelemään OSI-mallin kahta alinta kerrosta: fyysistä kerrosta ja siirtokerrosta. Tutkimuksessa ei ole käsitelty eri ratkaisujen tietoturvaa, elektronista suojautumista eikä autentikointimenetelmiä, elleivät ne ole teknisesti merkityksellisiä tapauksen käytettävyydelle.

Alla esitetyssä viitekehyksessä (kuva 1) kuvataan tutkimuksen kohteen asettumista Maavoimien tiedonsiirtoarkkitehtuuriin sekä tarpeita ja vaatimuksia, joita tutkittaville tapauksille asetetaan.



Kuva 1: Tutkimuksen viitekehys

1.4. Tutkimusmenetelmät

Tutkimus on lähtökohdiltaan kvantitatiivinen tapaustutkimus. Käytettävinä tutkimusmenetelminä ovat kirjallisuustutkimus, vaatimusmäärittely ja kenttäkokeet. Kenttäkokeiden suunnittelua edelsi kvalitatiiviseen sisällönanalyysiin perustuva kirjallisuustutkimus. Johtopäätökset kenttäkokeiden tuloksista perustuvat kvantitatiiviseen sisällönanalyysiin.

Tapaustutkimuksessa tutkitaan yksittäistä tapausta, tilannetta tai joukkoa tapauksia. Tapaustutkimuksessa ollaan usein kiinnostuneita prosessista. Tapausta tutkitaan suhteessa ympäristöönsä. Aineistoa kerätään useita metodeja käyttäen. Tapaustutkimuksen tavoitteena on usein tutkittavan ilmiön tarkka kuvailu.[8, s. 126] Vaikka tämä tutkimus ei ole yksittäisen tapauksen tarkka kuvailu, eikä tutkimuksessa keskitytä tutkittavien tapausten prosesseihin vaan tekniseen käytettävyyteen voidaan tutkimusta pitää tapaustutkimuksena, koska tutkittavat tapaukset on rajattu tarkasti.

Jyväskylän yliopiston kurssi- ja oppimateriaaliplone KOPPA:ssa julkaistulla tapaustutkimusta kuvaavalla verkkosivulla tapaustutkimuksen yleistettävyyttä kuvataan seuraavasti: *”Tapaustutkimusanalyysi ei siis pyri yleistettävyyteen sellaisin keinoin kuin esimerkiksi survey-tutkimus, mutta pyrkiessään ymmärtämään ja tulkitsemaan syvällisesti yksittäisiä tapauksia niiden erityisessä kontekstissa, se hakee tietoa ilmiöön liittyvän toiminnan dynamiikasta, mekanismeista, prosesseista ja sisäisistä ’lainalaisuuksista’ sellaisella tavalla, että tutkimuksen tuloksilla voidaan osoittaa olevan laajempaa sosiokulttuurista merkitystä ja siten jonkinlaista yleistettävyyttä tai siirrettävyyttä.”*[18]

Tutkimuksen käsitteiden määrittelyssä käytetään tutkimusmenetelmänä vertailevaa aineistolähtöistä sisällönanalyysiä ja koodausta. Koodauksessa lähteisiin on merkitty tutkimuksen kannalta oleelliset asiat. Koodauksen myötä löydetty tieto on luokiteltu ja järjestelty loogisesti. Koodauksen vuoksi aineiston löytäminen eri lähteistä on nopeampaa verrattuna tilanteeseen, jossa tekstiin ei olisi tehty minkäänlaisia merkintöjä [31].

Tässä tutkimuksessa on sisällönanalyysilla tiivistetty koodauksella merkittyjä teemoja lähdeaineistossa. Taistelukentästä on koottu eri lähteistä tietoja taistelukentän muutoksista sekä vaatimuksia tiedonsiirrolle ja johtamisjärjestelmälle. Lähiverkkojen tekniset kuvaukset ovat pääosin standardoituja eikä lähteiden sisällöissä ole juurikaan ristiriitoja. Verkkojen tekninen kuvaaminen on eri lähteissä hajanaista ja laajaa, joten tieto on koodauksen avulla teemoitettu ja tiivistetty ennen sen hyödyntämistä tutkimusraporttiin.

Teemat on jaettu tutkimuksen otsikon kahden aiheen alle. Taistelukentän teemat ovat suunnittelu, johtaminen ja tilannekuva. WLAN:n teemat on jaettu infrastruktuuriverkkoon ja Ad-Hoc-verkkoon sekä verkkojen suorituskykyihin.

Vaatimusmäärittelyn avulla vastataan tutkimuksen alatutkimuskysymyksiin. Tutkimuksessa määritellään toiminnalliset ja tekniset vaatimukset WLAN-standardien mukaisille verkoille ja laitteille kolmessa rajatussa tapauksessa. Tekniset vaatimukset perustuvat helposti mitattaviin suureisiin, joten vaatimusten määrittely on arvioitavissa laskennallisesti tarpeiden pohjalta.

Kenttäkokeilla on selvitetty tekniset ratkaisut ja asetukset, joilla tapaukset on toteutettavissa. Kenttäkokeilla on saatu vastaukset kysymyksiin voiko määritellyissä tapauksissa käyttää 802.11-standardin mukaista langatonta lähiverkkoa päätelaitteen liittämiseen. Kenttäkokeiden tulokset on kuvattu luvussa neljä.

Johtopäätökset on tehty hypoteettis – deduktiivisella päättelyllä. Suoritettujen kenttäkokeiden tuloksista on saatu vastauksia järjestelmien ominaisuuksista ja suorituskyvyistä. Ominaisuuksia ja suorituskykyjä on verrattu alatutkimuskysymysten vastauksina määritettyihin toiminnallisiin ja teknisiin vaatimuksiin. Tämän vertailun tuloksena on tehty johtopäätökset järjestelmien käytettävyydestä rajatuissa tutkimustapauksissa. Tutkimustulosten yleisempää käytettävyyttä ajatellen on pyritty tekemään myös johtopäätöksiä tutkituista kokonaisuuksista tutkimustapauksista poikkeavissa olosuhteissa.

1.5. Käsitteitä ja määritelmiä

Alla on määritelty tutkimuksessa käytettyjä käsitteitä, kuten ne tässä työssä ymmärretään. Käsitteet on määritelty, koska ne voivat olla moniselitteisiä tai lukijalle vieraita.

AdHoc-moodi termillä tarkoitetaan radioverkkoa, jossa ei ole tukiasemaa. Verkon solmut muodostavat verkon itsenäisesti.

AP-moodi (Access Point) termillä tarkoitettaan käyttötapaa, jossa verkossa on tukiasema. Verkon muut solmut liittyvät tukiasemaan.

Autentikointi tarkoittaa käyttäjän tunnistusta ja varmentamista.[14]

Ethernet on ensimmäinen standardoitu lähiverkkoratkaisu.[30]

Klusteri on jakautuneen verkon osa.[17]

Linkki on kahden solmun välinen yhteys.

OSI-malli on ISO:n (International Standardization Organisation) määrittämä standardi, joka kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemällä kerroksella. OSI-mallin alinta kerrosta, kerrosta 1 kutsutaan fyysiseksi kerrokseksi. Fyysinen kerros määrittelee lähinnä siirtotiet eli kaapeli-, tai radioyhteydet. Kerros 2, siirtokerros kehystää ylempien kerrosten tietoliikennepaketit fyysisen kerroksen siirtoa varten. Kerroksen 3, verkkokerroksen tehtävänä on yksinkertaistettuna valita mitä reittiä pitkin sanomat verkossa lähetetään. IP-protokolla kuuluu kerrokselle kolme. Kerros 4, kuljetuskerros vastaa luotettavasta yhteydestä päästä päähän. TCP- ja UDP-protokollat kuuluvat kuljetuskerrokselle. Kerros 5, istuntokerros tai yhteysjaksokerros vastaa siitä miten yhteys avataan, suljetaan ja ylläpidetään sekä avataan uudelleen sen katketessa. Tiedon salaaminen kuuluu kerrokselle viisi. Kerros 6, esitystapakerros vastaa oikeasta esitysmuodosta tiedonsiirron aikana. Tavoitteena on, että vastaanottaja ymmärtää saamansa tiedon. Tietojen pitää kulkea siten, että numerot tulostuvat numeroina ja kuvat kuvina. OSI-mallin ylimpänä kerroksena, kerroksena 7, on sovelluskerros. Sen tehtävänä on toimia linkkinä sovellukseen, joka siirrettyä tietoa tarvitsee. OSI-malli on kuvattu liitteessä 1.

Point-to-Point protokolla on tietoliikennetekniikassa käytetty termi, joka määrittelee kahden solmun välisen suoran yhteyden.

Päätelaite on laite, jolla käyttäjä käyttää sovelluksia ja palveluita.

Reititin on verkon komponentti, joka jakaa viestejä verkon osasta toiseen osoitetietojen perusteella.[14]

Silta (bridge) on kahden samantyyppisen verkon välinen yhdyskäytävä [14]. Silta on verkon komponentti, joka yhdistää verkon osia. Silta puskuroi ja suodattaa viestejä. Sillassa on kaksi porttia. Silta toimii OSI-mallin kerroksella kaksi.

Solmu (node) on radioverkossa toimiva itsenäinen laite. Solmu voi olla reititin tai päätelaite.

SSID on langattoman lähiverkon tunnus, jonka avulla verkot pystytään erottamaan toisistaan.[34]

Taistelukello määrittää esikunnan tavanomaisen työskentelyrytmin, joka perustuu tilanneilmoituksiin, esittelyihin ja kokouksiin sekä muihin esikunnan työskentelyyn vaikuttaviin päivittäisiin rutiineihin.

Taktinen Internet on taistelukentällä toimiva integroitu tiedonsiirtojärjestelmä, joka pohjautuu suurelta osin VHF- ja UHF-radioiden datansiirtokykyyn. Taktinen internet on jaettu toiminnallisesti kahteen osaan. Ylempi Taktinen Internet toimii lähinnä prikaati-tasolta ylöspäin ja alempi Taktinen Internet pataljoona-tasolta alaspäin.[15, s. 41-42]

TCP/IP-protokollapino on usean protokollan yhdistelmä, jossa alemmalla, eli verkkokerroksella toimiva IP (Internet Protocol) lähinnä määrittää päätelaitteiden osoitteet ja pakettien reitityksen. Verkkokerroksen päällä kuljetuskerroksella toimiva TCP (Transfer Control Protocol) vastaa kahden päätelaitteen tiedonsiirtoyhteydestä, pakettien kuljettamisesta, järjestämisestä ja uudelleen lähettämisestä.

Tilannekuva on kokonaisuus, joka perustuu tiedustelutietoihin vihollisen ryhmityksestä ja toiminnasta, omien joukkojen ryhmitykseen ja tehtävän suoritusvaiheeseen sekä tietoon naapurien ja ylemmän johtoportaan toiminnan vaikutuksista tilanteen kehittymiseen.

Tilannetieto on yksittäinen havainto mitä tapahtuu ja missä. Tilannekuva muodostuu tilannetiedoista. Tilannetieto voi olla arvokas analysoimattomanakin.[19]

Tilanneymmärrys koostuu tilannekuvasta ja kyvystä liittää se ympäröiviin olosuhteisiin sekä kyvystä hahmottaa toiminnan vaikutus kokonaisuuteen ja tilanteen kehittymiseen.

Toistin (repeater) on verkon komponentti, joka välittää viestin verkon osasta toiseen muuttumattomana.[14] Toistin toimii OSI-mallin kerroksella yksi.

Ulkoyhteydellä tarkoitetaan tässä tutkimuksessa lähiverkon ulkopuolista yhteyttä tai verkkoa johon lähiverkko on liitetty yhdestä solmusta.

WiFi Direct on WiFi alliancen tavaramerkki. Toiminnallisuus mahdollistaa laitteiden väliset Point to Point -yhteydet sekä AdHoc-tyyppiset moniyhteydet [38].

WDS-tekniikka tai AP + WDS moodi on tekniikka, jota käytetään infrastruktuuriverkon laajentamiseen. WDS-tekniikassa tukiasema toimii siltana.

2. TAISTELUTILAN MUUTOS

2.1. Taistelukenttä ja taistelutila

Perinteisen määritelmän mukaan taistelukenttä (battlefield) on kaksiulotteinen tila, jossa joukot kohtaavat taistellakseen. Termistä taistelukenttä ollaan siirtymässä termiin taistelutila (battlespace).[9, s. 61] Käsite taistelutila on määritelty julkaisussa *Maavoimien yhtymän suunnittelun ja päätöksenteon perusteet B-osa* vuodelta 2010: *”Taistelutila on yhtymän vastuualue ja sitä ympäröivä tila, jossa yhtymä voi omin, ylemmän johtoportaan ja naapureidensa menettelytavoin vaikuttaa viholliseen. Saatuaan tehtävän ja vastuualueen yhtymän komentaja hahmottelee mielessään tulevassa päätöksessään esittämänsä yhtymän taistelutilan, sen asettamat vaatimukset omalle operaatiolle, yhteistoimintatarpeet naapureiden kanssa ja esitykset ylemmälle johtoportaalle.”*[22]

Taistelutilaa on käsitelty Teemu Nurmelan esiupseerikurssin tutkimuksesta *Sotilaallisen kriisinhallintajoukon taistelutilaan vaikuttavat tekijät* vuodelta 2007 sekä Mika Huttusen teoksessa *Monimutkainen taktiikka* vuodelta 2010. Nurmela on viitannut Huttusen vuonna 2005 julkaistuun teokseen *Näkökulmia taktiikkaan – Taktiikan käsite ja taktiikan keinot tulkinnan kohteena*. Sekä Nurmela että Huttunen ovat verranneet eri määritelmiä kansainvälisiin määritelmiin. Näistä määritelmistä saadaan kuva taistelutilan moniulotteisuudesta, johon kuuluvat myös ilmatila ja sähkömagneettinen spektri [25, s. 10; 9, s. 61]. Huttunen on suomentanut yhdysvaltalaisesta strategian ja taktiikan sanakirjasta taistelutilan olevan *”alue, jossa taistelut, yhteenotot ja muut taktiset toiminnat toteutetaan. Taistelutila on moniulotteinen ja siihen kuuluvat maanpinta, maanpinnan alainen tila, ilmatila ja kyberneettinen tila (elektromagneettinen spektri)”.*[9, s. 61; 16, s. 23]

2.2. Johtamissodankäynti

Taistelukentän olosuhteet ovat muuttuneet tekniikan kehittyessä. Informaation merkitys sodan käynnissä on korostunut. Persianlahden sodan jälkeen 1990-luvulta alkaen on keskusteluihin noussut entistä voimakkaammin johtamissodankäynti. Konventionaalisin asein käytävistä taisteluista ei kuitenkaan ole luovuttu. Edelleen on sotia, joissa taistellaan mies miestä vastaan. Tällaisissa sodissa osapuolilla ei ole käytettävissään tietoverkkoja, eikä johtamissodankäynnillä informaatiohyökkäysten näkökulmasta ole vaikutusta sodan osapuolille.[13, s. 1]

Johtamissodankäynti käsitetään yleisesti informaationsodankäynnin osana. Käsitteitä on määritelty useissa eri lähteissä. Yhteistä määritelmille on, että informaatiosodankäynnissä pyritään vaikuttamaan informaatiosta riippuvaisiin päätöksentekoprosesseihin [7, s. 10]. Johtamissodankäynnin tavoitteena on erottaa joukot ja johtoportaat toisistaan [20, s. 9]. Yhteistä näille määritelmille on uhkaperusteisuus. Informaatiosodankäynti ja johtamissodankäynti nähdään ennen kaikkea vaikuttamisen kautta. Tavoitteena on vaikuttaa tiedon eheyteen ja käytettävyyteen. Tämä luo haasteen tietoverkkojen rakentamiselle, ylläpidolle ja hallinnoinnille. Tietoverkot pitää kyetä rakentamaan siten, että käytettävissä oleva tieto on luotettavaa, eheää ja oikea-aikaista [27, s. 166]. Käyttäjän pitää kyetä varmistumaan, että tietoa ei ole manipuloitu muuttamalla tai viivästyttämällä sitä.

2.3. Suunnittelun ja johtamisen vaatimukset johtamisjärjestelmälle

Taistelukentän ja sodan kuvan muutoksen myötä teknologinen kehitys on tuonut taistelukentälle johtamisjärjestelmät. Informaatioajan tekninen kehitys mahdollistaa toimet, joita ei ole voitu aiemmin toteuttaa. Kehityksen edetessä myös vaatimukset kasvavat, eikä johtamisjärjestelmä ole pelkästään mahdollisuus vaan se on nykypäivän taistelukentällä jo välttämättömyys. Johtaminen ei olisi mahdollista nykyisen kaltaisella konseptilla ilman toimivaa johtamisjärjestelmää. Johtamisjärjestelmän yksinkertainen englanninkielinen termi on kokonaisuuden ymmärtämisen kannalta kuvaava.[2] Command and Control system (C2) on vapaasti suomennettuna johtamis- ja valvontajärjestelmä. Suomen kielessä termi on vakiintunut muotoon johtamisjärjestelmä.

Suunnittelu on ollut olennainen osa sotatoimia jo varhaisesta historiasta lähtien. Suunnittelun tärkeys on korostunut joukkojen ja aseiden määrän lisääntyessä sekä sotatoimien monimutkaistuessa.[1, s. 42] Sotilaallisen suunnittelun ja teknologian kehittyessä on suunnittelussa siirrytty aiempaa nopeampaan rytmiin. Suunnittelulla tulee mahdollistaa taistelukellon mukainen johtaminen, tiedustelutietojen ja havaintojen mahdollistama ennakointi, raportointi sekä oikea-aikainen päätöksenteko. Suunnittelurytmi on usein 72 tuntia, mutta Yhdysvaltojen viimeaikaisista operaatioista saatujen kokemusten mukaan suunnitelmia on jouduttu päivittämään yhdeksän tunnin välein.[1]

Kiivas suunnittelurytmi ja aiempaa monipuolisemmat ja täydellisemmät suunnitelmat vaativat aiempaa suuremmat suunnitteluryhmät ja esikunnat. Usean henkilön osallistuessa suunnittelutyöhön suunnitelmien laatimisvastuut jaetaan eri henkilöiden kesken siten, että jokainen laatii omaa osuuttaan suunnitelmasta. Jotta suunnitelmat olisivat käytettävissä edellä kuvattujen vaatimusten mukaisesti, on suunnitelmien oltava riittävän laajalti käytössä, dokumentoitu ja säilytetty asianmukaisesti ja ennalta sovitusti.[1]

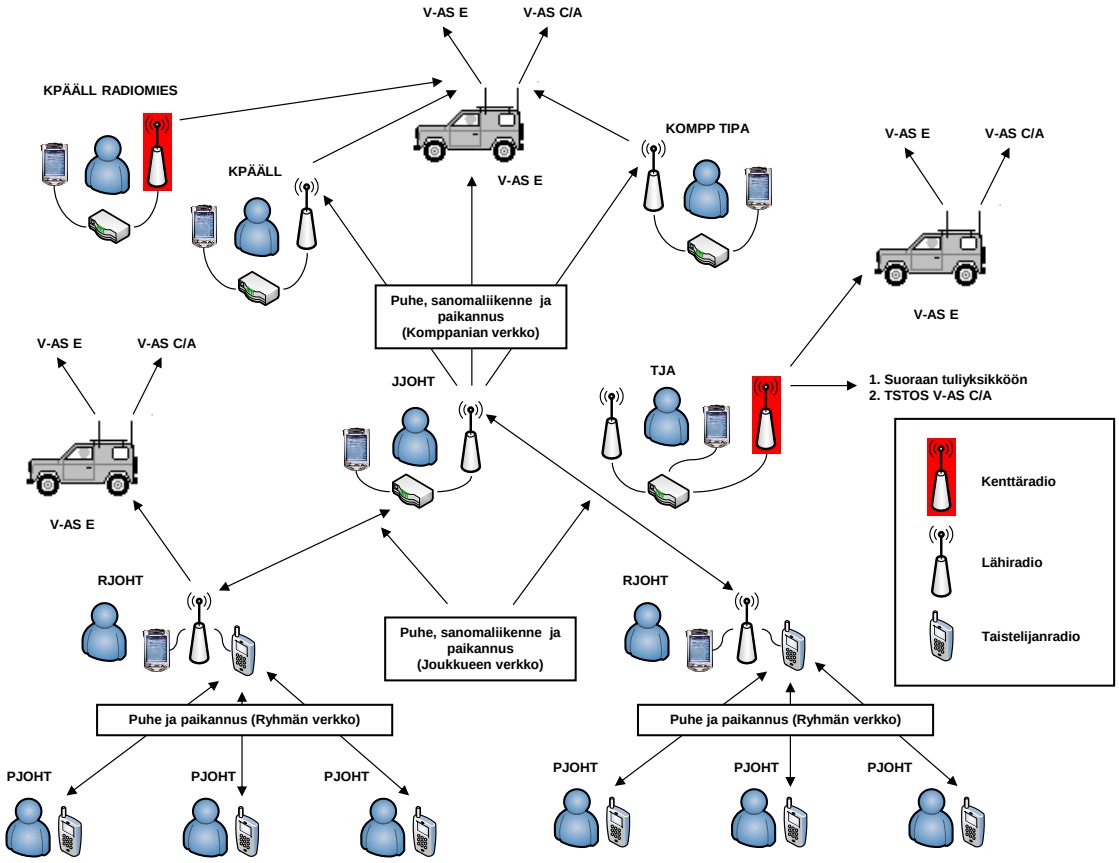
Tietojärjestelmien kehittyessä on edellisen kappaleen vaatimuksiin kyetty löytämään teknisiä ratkaisuja. Nykyisin suunnittelutyökaluina käytetään verkkopohjaisia sovelluksia ja tietojärjestelmiä. Suunnittelua kyetään tekemään yhdenaikaisesti tietokantapohjaisilla sovelluksilla. Tieto on dokumentoitu ja saatavissa käyttöoikeuksien salliessa.[1]

2.4. Pyrkimys reaaliaikaiseen tilannekuvaan

Nykyaikaisessa sodassa menestymisen edellytykset perustuvat komentajan riittävään tilanneymmärrykseen. Jotta komentaja voi saada riittävän tilanneymmärryksen, tulee hänellä olla kokemuksensa ja ammattitaitonsa lisäksi riittävän tarkka ja oikea-aikainen tilannekuva käytettävissään. Jos tilannekuva olisi täysin reaaliaikainen, olisi komentajalla käytössään koko ajan tarkka kuva siitä mitä taistelutilassa tapahtuu. Tähän ei kuitenkaan täysin päästä. Vihollistilannekuva koostuu eri puolilla taistelutilaa tehdyistä havainnoista, jotka ovat siirtyneet analysoitavaksi. Analysoinnin jälkeen on luotu arvio vihollisen toiminnasta. Toiminta aiheuttaa viiveitä sekä tiedonsiirrossa, käsittelyssä että analysoinnissa. Omien joukkojen tilannekuva ryhmityksen osalta rakentuu alla kuvatulla tavalla lähes reaaliaikaisesti. Siinäkin tulee huomioida tiedonsiirron aiheuttamat viiveet.

Maapuolustuksen liityntäverkot -konsepti kuvaa Maavoimien liityntäverkot ja niiden palvelut. Konseptin mukaan komppanian langattomaan lähiverkkoon kuuluu taistelijanradioita, lähiradioita ja dataradioita. Taistelijanradiot ovat lyhyen kantaman radioita, joilla saavutetaan enintään satojen metrien kantama. Lähiradiot ovat datansiirtoon kykeneviä kannettavia radioita. Joukkueet liittyvät komppanian viestiasemiin lähiradioillaan.[21, s. 17] Dataradiot on nimensä mukaisesti datansiirtoon tarkoitettuja radioita, joilla maapuolustuksen liityntäverkot -konseptin mukaan liitetään taisteluosastoja ja johtamispaikkoja [21, s. 9].

Ryhmänjohtajalla on lähiradion ja taistelijanradion lisäksi taistelunjohtojärjestelmän päätelaite. Ryhmän sisäinen tiedonsiirto perustuu taistelijanradioihin. Taistelijanradiot kykenevät siirtämään puheen lisäksi paikkatietoa. Tiedonsiirto ryhmästä ulospäin toteutetaan lähiradioilla. Partionjohtajien taistelijanradiot välittävät paikkatiedon ryhmänjohtajalle. Tiedot kootaan ryhmänjohtajan taistelijanpäätteeseen, johon muodostuu ryhmän tilannekuva. Ryhmänjohtajan taistelijanpäätteeltä kuva välitetään lähiradiolla joukkueenjohtajalle, josta edelleen komppanian päällikölle ja tilannepaikalle.[21, s. 17] Komppanian radioverkot on esitetty kuvassa 2.



Kuva 2: Komppanian johtamisjärjestelmä [21, s. 18]

Komppanian tilannepaikalta tieto välittyy johtosuhteiden mukaisesti ylemmän johtoportaan tilannekeskukseen, jossa tieto siirretään osaksi tilannekuvaa. Lisäksi komentajalla tulee olla riittävän ajantasainen tieto naapurien ja ylemmän johtoportaan toimista, jotta hän voi muodostaa tilanneymmärryksensä päätöksen teon perustaksi.

2.5. Johtopäätökset

Teknisen kehityksen myötä on tultu tilanteeseen, jossa informaation määrä on kasvanut huomattavasti perinteisiin sotiin verrattuna. Antiikin taisteluissa joukon komentaja näki koko taistelukentän ja kykeni luomaan ymmärryksen tilanteesta silmien edessä aukeavan kuvan perusteella. Nykyisin komentajalle luodaan tiedustelun tuottama kuva vihollisen toiminnasta, omien joukkojen välittämä kuva omasta ryhmityksestä sekä esikuntien rakentama malli siitä, kuinka tilannekuvan osat liittyvät suunniteltuun kokonaisuuteen.

Toisaalta vihollinen pyrkii kaikin keinoin vaikuttamaan tämän informaation saavutettavuuteen ja oikeellisuuteen. Rakennettavien verkkojen tulee siis kyetä välittämään oikeaa tietoa oikeaan aikaan ja oikeassa muodossa. Tiedon välittämiseen käytettävän verkon tulee olla rakenteeltaan robusti, kestävä ja varmennettu ja välityskyvyltään riittävä.

Haasteena tulevaisuuteen jää tilannekuvan välittämisessä syntyvien viiveiden minimointi.

Edellä kuvatuista muutoksista sekä johtamisen, suunnittelun tilannekuvan muodostamisen tarpeista saadaan muodostettua toiminnallisia, eli operatiivisia ja taktisia vaatimuksia johtamisjärjestelmille. Alla on lueteltu tutkijan lähdemateriaalin perusteella laatimia vaatimuksia, jotka langattomien lähiverkkojen on mahdollistettava:

- tilannetietojen välittäminen luotettavasti, eheänä, oikea-aikaisesti ja jatkuvasti
- kollaboraatiotyökalujen ja tietokantapohjaisten suunnittelusovellusten käyttö
- raporttien laatiminen ja muokkaaminen
- päätöksen tekeminen oikea-aikaisesti riittävään tilanneymmärrykseen perustuen
- käyttöoikeuksien ja näkymän rajaaminen.[2; 15; 19]

3. LÄHIVERKOT

3.1. Dataverkot

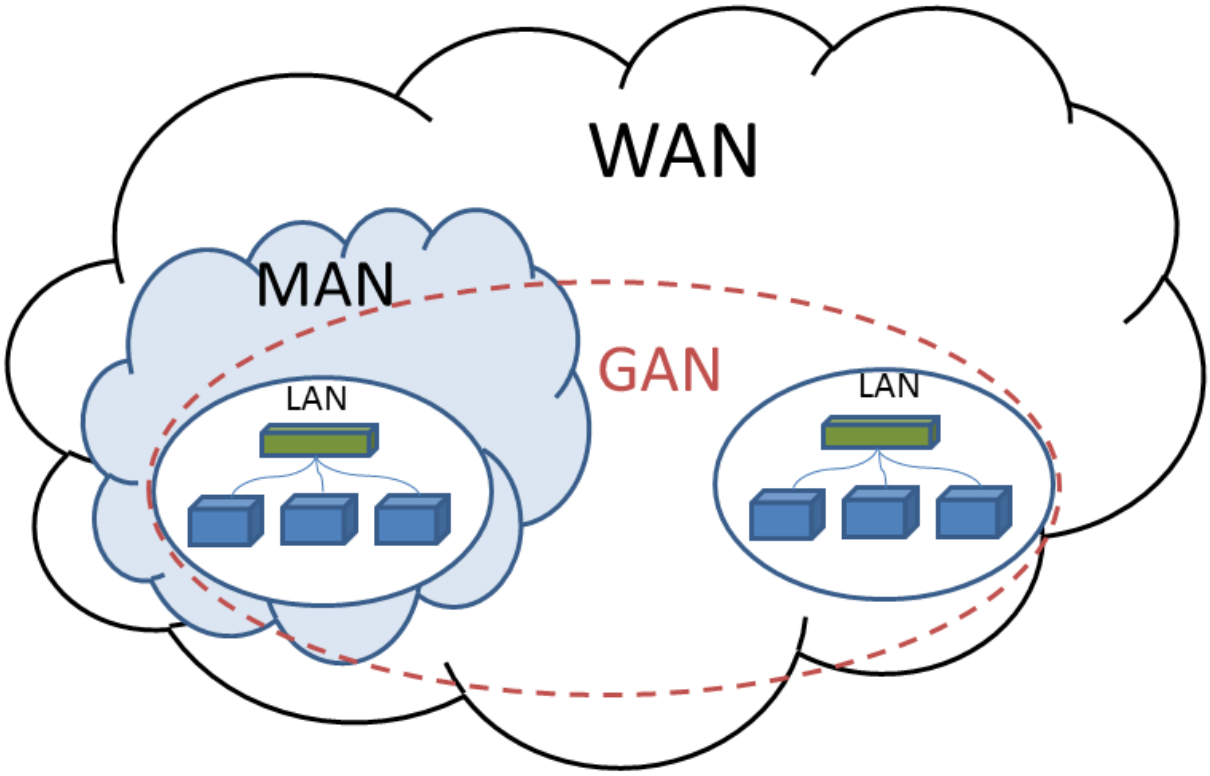
Lähiverkolla on perinteisesti tarkoitettu yrityksen tai organisaation rajattua dataverkkoa, johon on liitetty yrityksen tietokoneita ja oheislaitteita. Dataverkot on jaettu lähiverkkoihin (LAN), alueverkkoihin (MAN), etäverkkoihin (WAN) ja globaaliverkkoihin (GAN).[30, s. 11-12] Dataverkkojen keskinäinen suhde on esitetty kuvassa 3.

Lähiverkot on rakennettu rakennusten tai rakennusryhmän sisäisiksi nopeiksi rajatuiksi dataverkoiksi [30, s. 12]. Tutkijan IT-alan yrittäjänä hankkiman kokemuksen mukaan nykyisin langallisissa ethernet-verkoissa tiedonsiirtonopeus on käytännössä 100 Mbit/s, usein jopa 1 Gbit/s ja langattomissakin verkoissa vähintään 54 Mbit/s.

Havaintoa tukee 16.1.2014 tehty vertailu IT-tukkujen ja tunnettujen verkkokauppojen myydyimmistä ei-hallinnoitavista kytkimistä ja langattoman verkon reitittimistä. Yrityskäyttöön suunnatuissa ei hallinnoitavissa kytkimissä liitettäville laitteille tarkoitetut portit tukevat 10/100/1000 Mbit/s siirtonopeuksia. Osa kytkimistä sisältää kytkimien väliseen linkitykseen 10 Gbit/s portteja. Myydyimmät langattoman lähiverkon reitittimet tukevat 802.11b/g/n standardeja. Myydyimmät WLAN-reitittimet sisältävät 10/100 Mbit/s ethernet-portit laitteiden liittämiseen verkkokaapelilla.[3; 5; 24; 37]

Alueverkot ovat usein kaupunki- tai kampusalueen verkkoja, joissa on yhdistetty lähiverkkoja nopeilla yhteyksillä. Etäverkot ovat julkisten teleoperaattoreiden ylläpitämiä tiedonsiirtopalveluja. Verkot on toteutettu usein puhelinverkkoja varten rakennetuilla kaapeleilla. Globaaliverkot ovat yrityksen tai organisaation lähiverkkojen kokonaisuus, joka on yhdistetty alue- ja etäverkoilla.[30, s. 12]

Etäverkot käsitetään usein arkikielessä internetyhteytenä eli operaattoreiden tarjoamana laajakaista- tai mobiililaajakaistayhteytenä. Analogisen puhelinverkon jäätyä käytännössä historiaan on jo vuosia voitu keskittyä datan siirron tarpeisiin uusien yhteysvälien rakentamisessa. Kaapelointien kehittyessä ja varsinkin valokaapeliyhteyksien yleistyessä etäverkkojen datasiirtonopeudet ovat kasvaneet huomattavasti. Yleisimpien internetliittymissä käytettävien laajakaistatekniikoiden suurimmat teoreettiset siirtonopeudet ovat ADSL2+ maksimi 24/3 Mbit/s, VDSL2 100/100 Mbit/s, valokuitu 10/10 Gbit/s [26]. Ensimmäinen luku tarkoittaa latausnopeutta (download) ja jälkimmäinen luku lähetysnopeutta (upload).



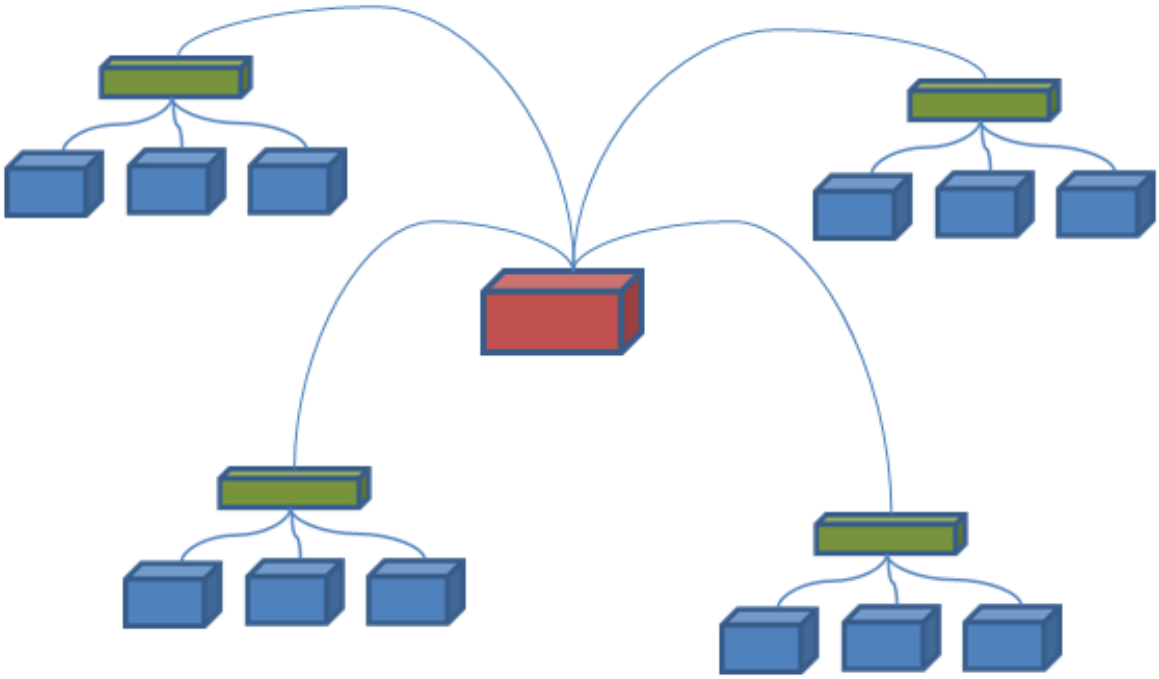
Kuva 3: Dataverkot perinteisen jaottelun mukaisina

3.2. Ethernet 802.3(x)

Ethernet on ensimmäinen standardoitu lähiverkkoratkaisu. IEEE:n standardi 802.3 on vuodelta 1985. 1990-luvulta alkaen on esitetty kilpailevia lähiverkkostandardeja, mutta ethernetin perusratkaisu on kuitenkin säilynyt. Ethernetin yksinkertaisista perusratkaisuista johtuen komponentit ovat varsin edullisia ja laitteita saa useilta valmistajilta.[30, s. 47]

Ethernetin mediavalikoima on kasvanut vuosien varrella. Alkuperäinen IEEE 802.3 mukainen lähiverkko on tiedonsiirtonopeudeltaan 10 Mbit/s ja siirtomediana käytettiin paksua koaksiaalikaapelia. Standardista käytettiin nimeä 10Base5. PC-työasemien liittämistä varten syntyi uusi ohut ethernet-liitäntä, jossa siirtomediana käytetään ohutta koaksiaalikaapelia ja lähetin/vastaanotinyksikkö saatiin integroitua verkkokortille. Standardi nimettiin 10Base2. Koaksiaalikaapelein toteutetut 10Base5 ja 10Base2 verkot olivat käytännössä kaapelilenkkejä, joihin päätelaitteet oli liitetty matkalle.[30, s. 48]

Nykyinen yleiskaapelointi on toteutettu parikaapelilla. Nousukaapelointina käytetään valokaapelia. Parikaapelin käyttö 802.3 standardissa on nimetty 10BaseT. Valokuitutoistin määriteltiin standardilla 10BaseF. Nykyiset ethernet-verkot ovat tähtiverkkoja, joissa päätelaitteet on kytketty parikaapelilla (CAT5, CAT6) keskittimeen, joka toimii toistimena. Keskittimet liitetään toisiinsa käytännössä parikaapelilla tai valokaapelilla. Ethernet-verkko voi näin olla kuvassa neljä esitetyn kaltainen useasta tähtiverkosta muodostuva tähtiverkko.[30, s. 49-51]



Kuva 4: Ethernet-verkon rakenne

3.3. WLAN 802.11(x)

Langaton lähiverkko (WLAN) poikkeaa ethernet lähiverkosta selkeimmin siirtotieltään. Langattomassa lähiverkossa siirtotienä toimii radioyhteys. WLAN on määritelty IEEE 802.11-standardeilla. Alla on kuvattu pääpiirteissään tutkijan näkemyksen mukaan langattomien lähiverkkojen kehityksen ja käytettävyyden kannalta merkityksellisimmät 802.11 perheen standardit. Standardeiksi valittiin yleisimmin käytetyt 802.11b/g/n sekä niihin johtaneet alkuperäinen 802.11 sekä 802.11a. Kehitteillä olevista standardeista tutkija näkee tutkimuksen tapauksia eniten tukevaksi 802.11s standardin (MESH). MESH on eräänlainen AdHoc- ja AP-verkkojen yhdistelmä.

802.11s ei standardina määritä tiedonsiirtokykyä vaan se on MAC-kerroksen laajennus. 802.11s tarvitsee tiedonsiirtoon 802.11a, 802.11b, 802.11g tai 802.11n standardia.[11]

IEEE 802.11 standardi on julkaistu vuonna 1997. Standardin mukaisissa verkoissa käytetään ISM taajuusalueen taajuuksia 2400,000–2483,500 MHz. Alkuperäisen standardin mukaisen verkon tiedonsiirtonopeus on 1–2 Mbit/s.[33, s. 165] ISM-kaistan etuna on, ettei standardinmukaisille teollisuus-, tiede- ja lääketieteellisille laitteille tarvita käyttölupaa. Taajuusalue on käytettävissä eri puolilla maailmaa. Taajuuskaista on kuitenkin samasta syystä myös muiden laitteiden, kuten mikroaaltouunien käytössä.[30, s. 114-115]

IEEE 802.11 standardin mukaisen 2.4GHz taajuusalue on jaettu neljääntoista kaistaan. Kaistoista 1–11 on käytössä Euroopassa ja Pohjois-Amerikassa, kanavat 12 ja 13 Euroopassa ja kanava 14 ainoastaan Japanissa.[12, s. 566] Usein kuitenkin Euroopassakin myytävissä laitteissa on käytössä vain kanavat 1–11. Kanavat ja niiden keskitaajuudet on esitetty taulukossa 1.

Taulukko 1: 802.11b ja g verkkojen kanavat ja keskitaajuudet [12, s. 566]

Kanava	Keskitaajuus
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz
12	2467 MHz
13	2472 MHz
14	2484 MHz

Samassa tilassa olevien verkkojen taajuudet voivat häiritä toisiaan ja vaikuttaa verkon suorituskykyyn. Verkot tulisi asettaa eri kanaville. Jos käytössä on vain yksitoista kanavaa, on kolmella verkolla suorituskyvyn kannalta optimaalinen ratkaisu käyttää kanavia 1, 6 ja 11.

802.11b julkaistiin vuonna 1999. Standardin merkittävin etu alkuperäiseen 802.11 standardiin on 11 Mbit/s tiedonsiirtonopeus. 802.11b laajennus toimii alkuperäisen standardin mukaisella 2.4 GHz taajuudella. 802.11a julkaistiin yhtä aikaa 802.11b:n kanssa. 802.11a:n mukainen taajuus on kuitenkin korkeampi 5 Ghz (5.15–5.35 Ghz).[23] Standardin mukainen teoreettinen tiedonsiirtonopeus on 54 Mbit/s käytännön siirtonopeuden jäädessä kuitenkin 22 Mbit/s.

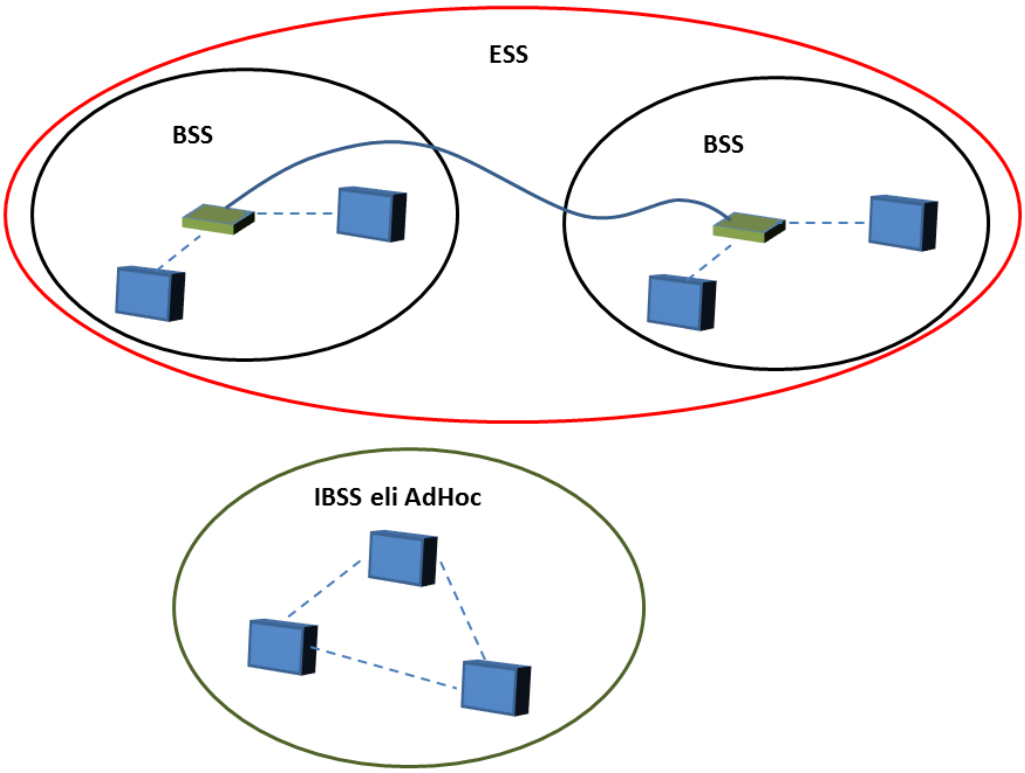
802.11g julkaistiin vuonna 2003. Standardin määrittämä taajuus on 2.4 GHz tiedonsiirtonopeuden ollessa 54 Mbit/s. Vuonna 2009 julkaistiin 802.11n. Standardin mukaiset laitteet toimivat sekä 2.4 että 5 GHz taajuuksilla.[23] Standardi määrittelee moniantennitekniikan (MIMO). Standardissa on tavoiteltu jopa 600 Mbit/s tiedonsiirtonopeutta. 802.11n mahdollistaa yhdellä antennilla 150 Mbit/s tiedonsiirtonopeuden. Antennien määrä kertaa maksinopeuden, joten neljällä antennilla voidaan päästä 600 Mbit/s tiedonsiirtonopeuteen.[29, s. 19] Standardi on osittain yhteensopiva aiempien standardien kanssa. Tällöin on kuitenkin rajoittavana tekijänä vanhemman standardin mukainen suorituskyky.

Tammikuussa 2014 hyväksyttiin standardi 802.11ac. Standardi tukee MIMO-tekniikkaa ja mahdollistaa sekä 2.4 GHz että 5 GHz taajuusalueiden käytön. 802.11ac-standardi mahdollistaa teoriassa 1600 Mbit/s siirtonopeudet sekä 80 MHz ja jopa 160 MHz kaistanleveyden.[10] Standardin laitteita on yleisesti myynnissä, mutta se ei ole vielä syrjäyttänyt aiempia standardeja. Kuten aiemmatkin standardit, tukevat 802.11ac laitteet vanhempia standardeja, mikä osaltaan hidastaa aiempien standardien mukaisten laitteiden poistumista käytöstä.

3.4. Langattoman lähiverkon topologia

Langaton lähiverkko voi olla infrastruktuuriverkko, jossa verkko rakentuu tukiaseman (AP, Access Point) ympärille. Yksinkertaisimmillaan tällaisessa verkossa on tukiasema ja liittyjä. Tällaisesta verkosta käytetään termiä BSS (Basic System Set). Toinen arkkitehtuuri langattomalle lähiverkolle on IBSS (Independent BSS). Arkkitehtuurista käytetään yleisesti nimitystä AdHoc-verkko. AdHoc-verkossa ei ole tukiasemaa, vaan liittyjät muodostavat verkon.[12] Tässä tutkimuksessa langattomien lähiverkkojen arkkitehtuurista käytetään termejä AP-moodi ja AdHoc-moodi. Kolmas verkkomalli liittyy MESH-teknologiaan, joka on eräänlainen AP- ja AdHoc-moodien yhdistelmä.

Infrastuktuuriverkkoa voidaan laajentaa liittämällä tukiasemia toisiinsa. Tällöin erilliset BSS-verkot muodostavat ESS-verkon (Extended Service Set). ESS-verkossa voi olla liittyjiä rajoittamattomasti, kun kaikki liittyjät ovat liittyneet kyseisen ESS-verkon tukiasemiin.[12, s. 26]

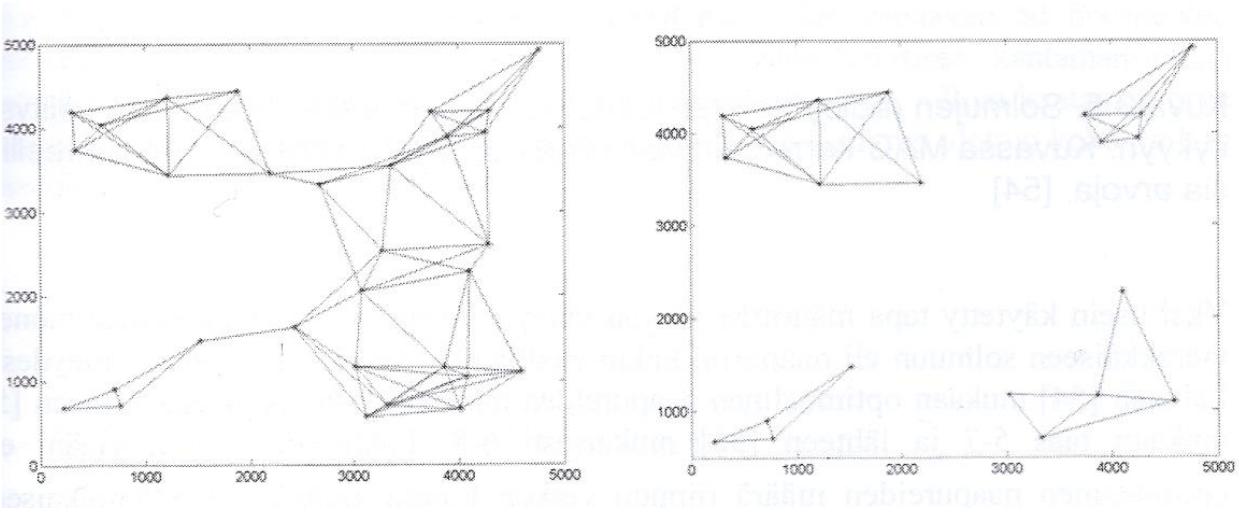


Kuva 5: Wlan-verkkojen topologiat

AdHoc-verkot ovat rakenteettomia verkkoja, joissa ei ole keskitettyä kontrollia. Verkot muodostuvat automaattisesti sekä kykenevät konfiguroitumaan automaattisesti yksittäisten solmujen tuhoutuessa tai niiden välisten yhteyksien katketessa. Verkkoon liittyvät solmut kykenevät paitsi lähettämään ja vastaanottamaan viestejä myös välittämään niitä.[17, s. 5-7]

AdHoc-verkkoa käytetään tilanteissa, joissa verkon rakentaminen on väliaikaista ja liittyjät vaihtuvat. AdHoc-verkossa on oltava vähintään kaksi laitetta. Verkon solmujen enimmäismäärää ei ole standardissa rajoitettu.[12, s. 25, 42] Solmujen määrän rajaa käytännössä verkon kapasiteetti, joka jakautuu kaikkien verkkoa käyttävien solmujen kesken. Kapasiteettia kuluttavat radiotien häiriöt, välitettävä liikenne, kontrolliliikenne ja kehyksen vaatima kaista.[17, s. 87]

AdHoc-verkon yhteydessä puhutaan yhteydellisyydestä, jolla tarkoitetaan verkon solmujen yhteyttä toisiinsa. Yhteydellisessä verkossa kaikki solmut voivat lähettää viestejä toisilleen. Mikäli verkko jakautuu jonkin tai joidenkin linkkien katketessa verkosta muodostuu erillisiä klustereita.[17, s. 48-49] Kuvassa 6 on kuvattu verkon yhteydellisyys normaalitilanteessa sekä klusteroinut verkko 30% tappioiden jälkeen.



Kuva 6: AdHoc-verkon yhteydellisyys normaalitilanteessa ja 30% tappioiden jälkeen [17, s. 49]

AdHoc-verkon kapasiteettiin vaikuttaa verkon koko eli solmujen määrä, solmujen välisten yhteyksien välitysnopeus sekä verkon välityskyky yhtä solmua kohden. Mikäli solmut ovat jakautuneet satunnaisesti koko verkon alueelle, yhtä solmua kohden jäävä kapasiteetti voidaan laskea alla olevalla kaavalla:

$$T_{hput} = W/\sqrt{n\log n}$$, jossa

T_{hput} = välityskyky yhtä solmua kohden

W = solmujen välisten yhteyksien datanopeus

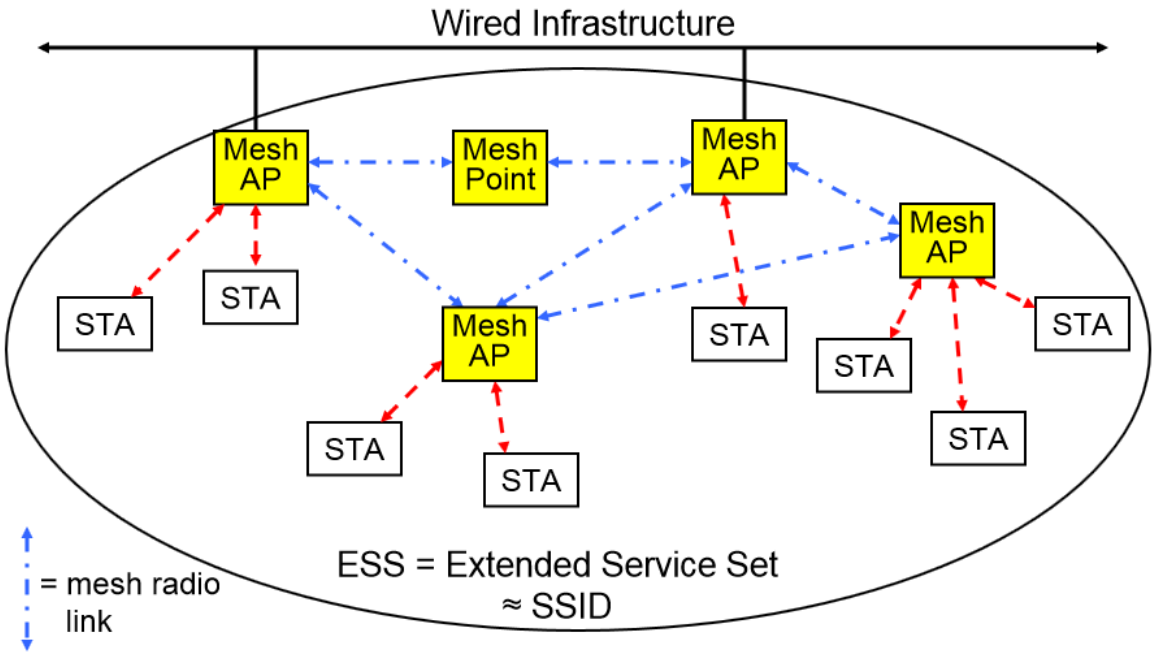
n = verkon solmujen määrä.[17, s. 88]

Verkon solmujen sijoittuessa optimaalisesti ja solmujen välisen radioliikenteen ollessa optimaalinen voidaan päästä tilanteeseen, jossa kapasiteetti voidaan laskea kaavalla:

$$T_{hput} = W/\sqrt{n}$$ [17, s. 88]

Jos verkossa on 10 solmua ja solmujen välinen siirtoyhteys on nopeudeltaan 2 Mbit/s, saadaan yksittäisen solmun siirtonopeudeksi 707 kbit/s. Solmujen määrän noustessa viiteenkymmeneen on siirtonopeus enää 283 kbit/s. Petteri Kuosmanen on kertonut kahdeksan solmun koeverkossa yhden solmun kapasiteetin olleen kuitenkin vain $W/n^{1,68}$. Kymmenen solmun verkossa siirtoyhteyksien ollessa 2 Mbit/s jää yhden solmun kapasiteetiksi vain 61 kbit/s. Mitattu kapasiteetti oli alle kymmenen prosenttia teoreettisesta kapasiteetista. Laitteiden määrän lisääntyessä yksittäisen solmun kapasiteetti pienenee.[17, s. 88-89]

AdHoc- ja MESH-termit tarkoittavat usein verkkoja, joiden rakenne voi muuttua dynaamisesti ja solmut voivat muodostaa yhteyksiä itsenäisesti [15, s. 102]. MESH-verkkoja kehitetään standardien 802.11s ja 802.16j (WIMAX) yhteistyössä. MESH-verkkoihin on yhdistetty myös 802.15 (Bluetooth). MESH-verkoissa solmut liittyvät MESH-tukiasemiin, jotka perinteisestä mallista poiketen liittyvät toisiinsa radiolinkeillä. MESH-tukiasemat tarjoavat siis tukiasemaverkon paikallisille tai alueellisille liityntäverkoille. MESH-verkossa liikkuminen onnistuu yhteyden katkeamatta.[28, s. 95] MESH-verkon topologia AP-moodissa on esitetty kuvassa 7.



Kuva 7: MESH-verkon topologia [4]

3.5. Johtopäätökset

802.11-standardia on kehitetty tietotekniikan kehittyessä. Myös tarpeiden muuttuminen vaikuttaa standardin kehittämiseen. Alkuperäinen 802.11-standardi määrittää taajuusalueeksi 2.4 GHz, laajennus 802.11a toi uutena 5 GHz:n taajuusalueen. 802.11g lisäsi siirtonopeutta 2.4 GHz:n taajuusalueelle. Laajennuksesta 802.11n eteenpäin ovat standardit tukeneet molempia taajuusalueita. Standardin laajennukset ovat tuoneet mukanaan parannuksia, jotka mahdollistavat paremmat siirtonopeudet ja suuremmat taajuuskaistat. Lisäksi on vähemmän tunnettuja standardin laajennuksia, jotka vastaavat spesifiseen tarpeeseen, kuten 802.11s, joka on luotu lähinnä MESH-tekniikan mahdollistamiseksi.

Yleisesti standardin laajennukset tukevat vanhempia versioita ja laajennuksia. Näissä tilanteissa huomioitavaa on verkon suorituskyvyn rajoittuminen alinta tasoa edustavan komponentin mukaan. Kun verkon tulee vastata ennalta määritettyihin vaatimuksiin, kuten tilannekuvan välittämiseen, on verkon rakenteessa ja komponenteissa huomioitava tilannekuvan siirtämiseen tarvittava siirtonopeus ja kaistanleveys. Käytettävällä taajuusalueella ja antennitekniikalla on vaikutusta yhteysetäisyyksiin. Ne vaikuttavat kantamaan ja häiriöiden sietoon.

Jos tilannekuva siirretään ascii-pohjaisina viesteinä, ei siirtonopeudelle ole suurta vaatimusta. Mikäli on tarve siirtää word- tai powerpoint-dokumentteja tai kuvatiedostoja kasvaa tiedonsiirtonopeuden tarve.

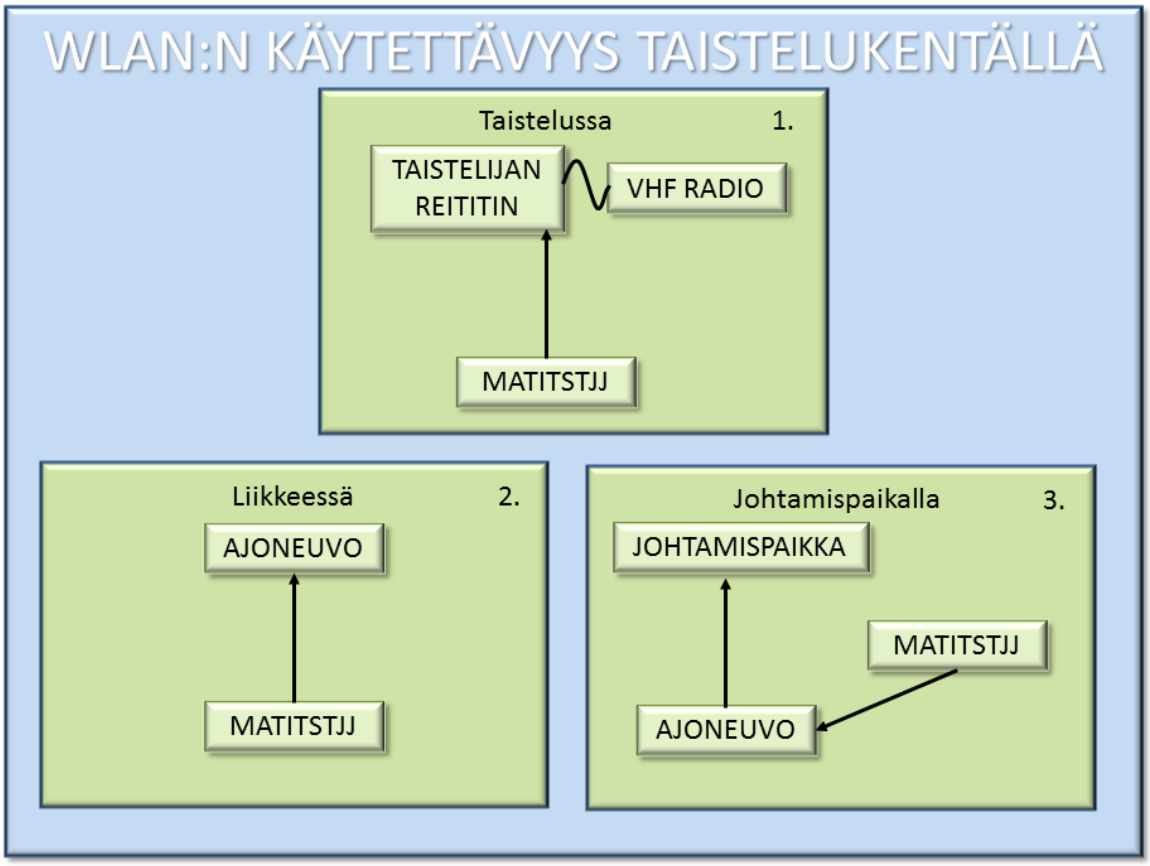
Verkkoa suunniteltaessa käytettävillä solmuilla on merkitystä verkon siirtonopeudelle ja käytettävälle taajuusalueelle. Verkon päätelaitteiden tulisi siis tukea uusinta hyväksyttyä standardia, jotta verkosta voidaan saada suurin mahdollinen hyöty. Tutkimuksen tekohetkellä laitteiden tulisi tukea 802.11n tai 802.11ac standardia. 802.11n ja 802.11ac standardit tukevat molempien taajuusalueiden käyttämistä sekä MIMO-tekniikkaa. 802.11ac mahdollistaa tutkimuksen tekohetkellä leveimmän taajuuskaistan ja korkeimman siirtonopeuden WLAN-verkoissa.

Verkkotopologiassa ja käytettävissä moodeissa suurimmat erot ovat hallittavuudessa ja verkon rakenteen dynaamisuudessa. AP-moodissa verkon hallintaan on teknisesti paljon mahdollisuuksia. Tukiasemien asetuksilla voidaan vaikuttaa esimerkiksi verkkoon liittyvien solmujen oikeuksiin, rajoittaa ja reitittää liikennettä. AdHoc-moodissa verkko muodostuu automaattisesti vähintään kahden solmun ollessa kantaman sisällä samoilla asetuksilla. Verkon muutokset tapahtuvat dynaamisesti vaikuttamatta verkossa olevien muiden solmujen toimintaan. MESH-tekniikalla näitä ominaisuuksia voidaan osittain yhdistää. Dynaamiset AdHoc-verkot voidaan yhdistää toisiinsa radiolinkeillä. Solmut, joiden kautta verkot yhdistetään voivat tuoda AdHoc-verkkoon ulkoyhteyden ja toimia tukiasematyyppisesti hallittavina laitteina.

Käytetty lähdeaineisto ei tunne 802.11s ja 802.11ac yhteensopivuutta [4]. Sen voidaan olettaa johtuvan siitä, että standardi 802.11ac on julkaistu käytännössä vuoden 2014 alussa eikä se ole ehtinyt käytössä olevaan lähdemateriaaliin. Koska 802.11s on MAC-kerroksen laajennus, se ei vaikuta OSI-mallin fyysisen kerroksen toimintaan ja se tukee todennäköisimmin myös tulevia standardin 802.11 laajennuksia siirtokapasiteetista ja taajuudesta riippumatta.

4. PÄÄTELAITTEEN LIITTÄMINEN WLAN:LLA

Koska tutkittava aihe on laaja, tutkittavat tapaukset on rajattu kuvassa 8 esitettyihin tapauksiin. Tapausten tutkiminen herätti useita pienempiä kysymyksiä. Ilman näitä kysymyksiä ei tutkimuksessa olisi voitu saavuttaa vastauksia johdannossa esitettyihin tutkimuskysymyksiin ja päätutkimusongelmaan. Kysymykset on kirjattu alalukujen alkuun selvittämään kuinka tapauskohtaiset tutkimustulokset on saavutettu. Tapauksia tutkittiin kenttäkokeilla. Kenttäkokeiden tutkimuskysymykset on esitetty kenttäkoeraportissa, joka on liitteenä 2.



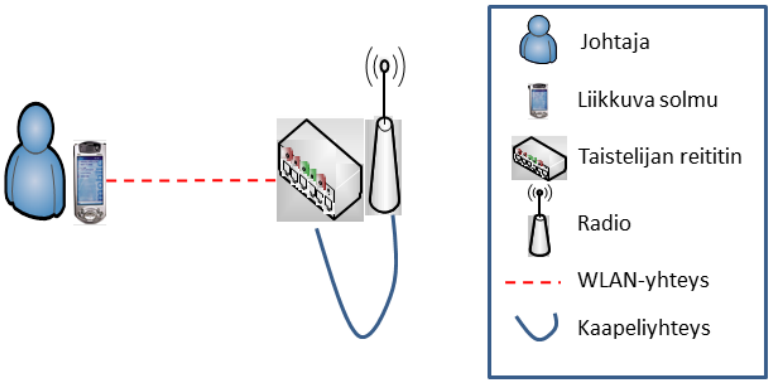
Kuva 8: Tutkimuksen tapaukset

Ensimmäisessä tapauksessa päätelaite on liitetty taistelijan reitittimeen WLAN-yhteydellä. Taistelijan reititin on liitetty VHF-radioon kaapelilla. Toisessa tapauksessa tutkitaan tilannetta, jossa päätelaite kytkeytyy ajoneuvon langattomaan lähiverkkoon. Kolmannessa tapauksessa päätelaite on liittyjänä ajoneuvon langattomassa lähiverkossa tilanteessa, jossa ajoneuvo liittyy johtamispaikan langattomaan lähiverkkoon. Tapaus poikkeaa kahdesta edellä mainitusta, koska ajoneuvon WLAN-laitteilla on kaksi roolia. Ajoneuvon tulee tarjota yhteys päätelaitteelle ja toisaalta liittyä johtamispaikan verkkoon.

4.1. Päätelaite liittyjänä taistelijan reitittimessä

Tapauksessa johtaja on joukkonsa osana taistelukentällä. Johtajalla on päätelaite, jonka avulla hän saa tilannepäivityksiä esimiehiltään. Toisaalta päätteelle kerätään alaisten taistelijanradioista sijaintitiedot, joista koostetaan tilannekuva omista joukoista edelleen lähetettäväksi esimiehelle ja tilannepaikoille.

Tutkittavassa tapauksessa päätelaite liitetään WLAN-standardin mukaisesti VHF-radioon kytkettyyn taistelijan reitittimeen. Yksinkertaisimmillaan liittäminen tapahtuu kahden WLAN-radion välisellä Point to Point -yhteydellä. Tapaus on kuvattu kuvassa 9.

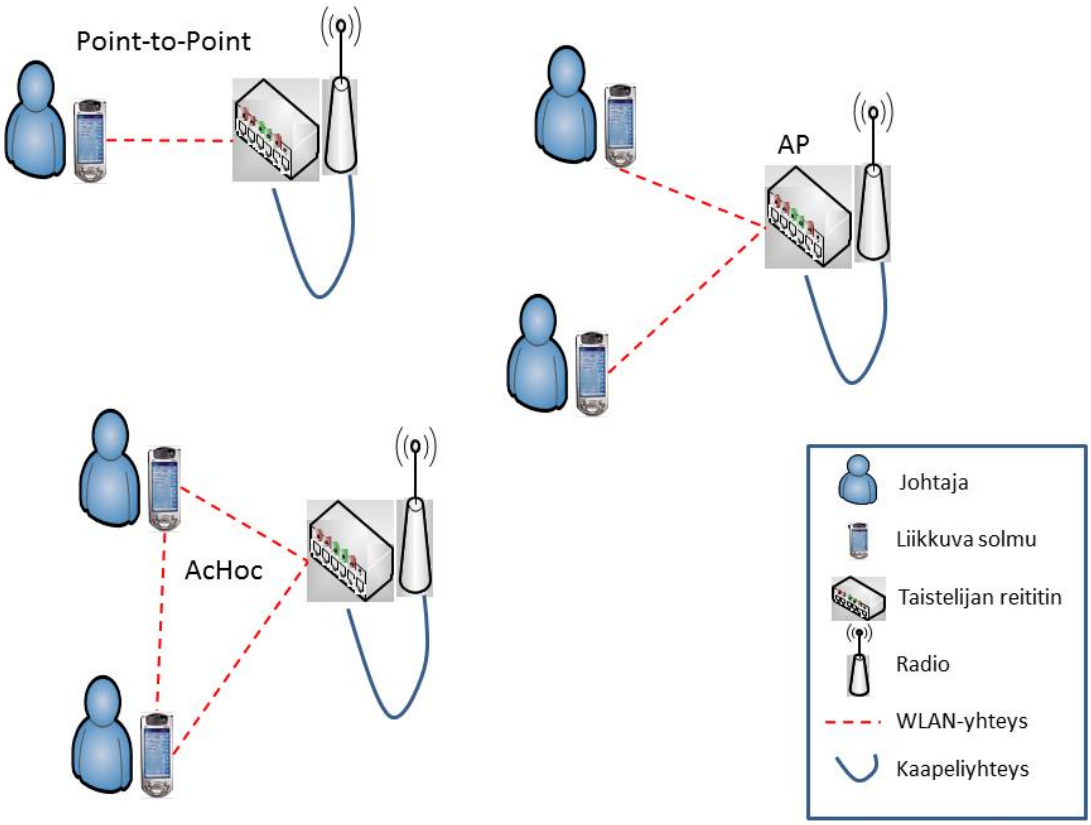


Kuva 9: Tapaus 1

Yhteys voidaan toteuttaa infrastruktuuriverkkona, jolloin taistelijanreititin asetetaan AP-moodiin. Johtajan päätelaite liittyy tukiasemaan asiakkaana (client). Ratkaisussa alueelle saapuvat muut päätelaitteet, joilla on WLAN-yhteys voivat liittyä tukiasemaan asiakkaina. Päätelaitteiden väliset viestit kulkevat tukiaseman kautta. Päätelaitteet eivät ole riippuvaisia toisistaan.

Yhteys voidaan toteuttaa myös AdHoc-verkkona. AdHoc-verkossa solmut ovat samanarvoisia. Alueelle tulevat päätelaitteet voivat liittyä verkkoon itsenäisesti. Laitteiden väliset viestit kulkevat suoraan laitteelta toiselle. Jos laitteet eivät ole yhteydessä toisiinsa, muut verkossa olevat laitteet välittävät viestin.

Vaihtoehdot päätelaitteen liittämiseen ja verkon laajentamiseen on esitetty kuvassa 10.



Kuva 10: Päätelaitteen liittäminen taistelijan reitittimeen

Pysyttäessä OSI-mallin kahdella alimmalla kerroksella voidaan tapauksen rajoitteet yksinkertaistaa käsittämään päätelaitteen käytössä oleva kaista ja verkon nopeus. Yksittäisen solmun käytössä oleva siirtonopeus pienenee yhteysetäisyyden kasvaessa ja verkon solmujen määrän lisääntyessä luvussa kolme kuvatulla tavalla. Verkon kantamaa ja maksimaalista yhteysetäisyyttä voidaan arvioida laskemalla kohde-etäisyydelle tuleva teho vähentämällä laskennallinen vaimennus lähetystehosta.

Vapaan tilan vaimennus saadaan laskettua alla olevalla kaavalla. Kaavaa on yksinkertaistettu alkuperäisestä Friisin yhtälöstä olettamuksella, että käytössä on isotrooppiset antennit sekä lähettimessä että vastaanottimessa. Tällöin teho leviää ympäristöön pallomaisesti. Isotrooppisen antennin vahvistus on 1.[32]

$$L_P = \left(\frac{4\pi d}{\lambda}\right)^2$$

L_p = lähetystehon ja vastaanotetun tehon suhde

d = etäisyys

λ = aallonpituus.

Jotta radioaalto voi edetä täysin vapaassa tilassa, lähetin- ja vastaanotinantennien välisen Fresnelin ellipsoidin 1. vyöhykkeen tulee olla vapaa esteistä. Tämän vaatimuksen saavuttaminen on mahdollista nostamalla antennit riittävän korkealle. Fresnelin ellipsoidin 1. vyöhykkeen säteen ja yhteysetäisyyden suhde saadaan laskettua kaavalla:

$$h = \sqrt{\lambda(d1 * d2)/(d1 + d2)}$$

h = fresnelin ellipsoidin 1. vyöhykkeen säde mittauskohdassa (m)

$d1$ = etäisyys mittauskohtaan antennista 1 (m)

$d2$ = etäisyys mittauskohtaan antennista 2 (m)

λ = aallonpituus.

Laskettaessa esteistä vapaan fresnelin ellipsoidin 1. vyöhykkeen sädettä voidaan kaavaa yksinkertaistaa. Esteettömän ellipsoidin suurin halkaisija on keskellä ellipsoidia, eli yhtä kaukana molemmista antenneista. Saadaan $d1 = d2$. Yhteysetäisyys $D = d1 + d2$. Aallon pituudesta voidaan laskea taajuus kaavalla:

$$\lambda = c / f$$

λ = aallonpituus

c = valonnopeus (m/s)

f = taajuus.

Yllä kuvatuilla yksinkertaistuksilla kaava voidaan kuvata muotoon:

$$r = 8{,}657 * \sqrt{D/f}$$

r = ellipsoidin säde keskellä (m)

D = antennien välinen etäisyys (km)

f = taajuus (GHz).

Fresnelin ellipsoidin säde on samalla antennin vähimmäiskorkeus tavoiteltaessa täysin vapaata fresnelin ellipsoidin 1. vyöhykettä. Laskettaessa antennikorkeutta 5 m yhteysvälille 2,4 Ghz WLAN-yhteydelle saadaan tulokseksi 0,95 m.

$$r = 8{,}657 * \sqrt{0{,}005 * 2{,}4}$$

Vapaan tilan etenemisenä antennien tulisi olla noin metrin korkeudella esteistä, kuten maan pinnasta. Seisovilla ihmisillä selässä pidettävä radio ja kädessä pidettävä päätelaite täyttää vaatimuksen. Yleisesti hyväksytään, että fresnelin ellipsoidin 1. vyöhykkeestä 60% on esteetöntä, suositeltavaa olisi pyrkiä saamaan vyöhykkeestä esteettömäksi 80% [6].

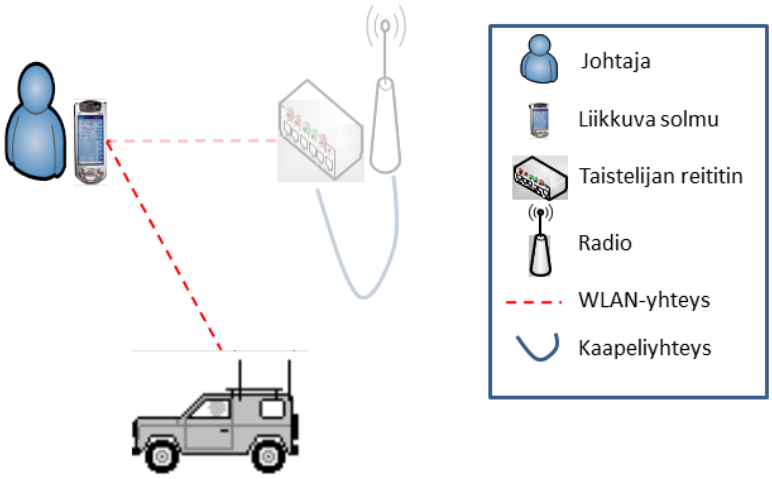
Tulos ei tarkoita, että yhteys ei toimisi matalammilla antennikorkeuksilla. Antennien ollessa matalammalla ei voida enää käyttää vapaan tilan vaimennusta. Maanpinta ja muut esteet vaimentavat signaalia huomattavasti vapaan tilan vaimennusta enemmän. Laskennallinen teho vastaanottimessa on pienempi kuin yllä on laskettu.

Käytännön kantama metsämaastossa on usein kuitenkin paljon laskennallista tulosta heikompi. Puuston ja olosuhteiden aiheuttamaa vaimennusta ei kyetä arvioimaan riittävällä tarkkuudella. Mittaustuloksia löytyy eri tutkimuksista, mutta tulos riippuu aina käytetyistä päätelaitteista, antenneista ja mittauspaikan olosuhteista, joten tulosten yleistettävyys on heikko.

Tapauksessa WLAN-yhteydellä pyritään korvaamaan radion ja päätelaitteen välinen kaapeli. Vaatimukseksi asetetaan kahden poteron välinen etäisyys, etäisyys johtajasta radiomieheen. Yhteysväli on enintään viisi metriä. WLAN-yhteyden on mittauksissa todettu mahdollistavan kolmenkymmenen metrin yhteyden sisältä ikkunan läpi ulos 802.11g standardin mukaisessa verkossa [35]. Voidaan siis todeta WLAN-yhteyden kantaman riittävän vaadittavalle yhteysvälille.

4.2. Päätelaite liittyjänä ajoneuvon langattomassa lähiverkossa

Tapauksessa johtaja on ajoneuvossa, jossa on langaton lähiverkko. Johtaja liittää päätelaitteensa ajoneuvon WLAN-verkkoon. Tapauksessa tutkitaan onko verkkoon liittyminen mahdollista. Tutkitaan onko mahdollista liittyä asetuksilla, jotka ovat käytössä ensimmäisessä tapauksessa. Tutkitaan aiheutuuko verkon vaihtamisesta viivettä ja yhteyskatkoksia. Tapaus on esitetty kuvassa 11.

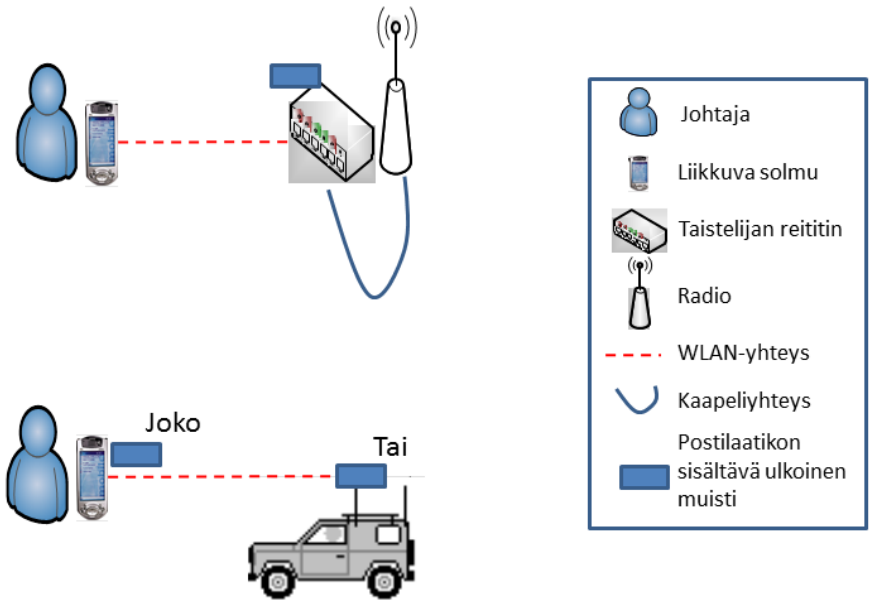


Kuva 11: Tapaus 2

Päätelaite voidaan liittää ajoneuvon reitittimeen, kuten se liitettiin taistelijanreitittimeen ensimmäisessä tapauksessa. Yhden päätelaitteen tapauksessa kyseessä on Point to Point -yhteys. Ajoneuvon reititin voidaan asettaan AP-moodiin, jolloin päätelaite liittyy verkkoon tai ajoneuvon reititin ja päätelaite voivat muodostaa AdHoc-verkon.

Tapaukseen liittyy myös johtajan sähköpostilaatikon sijainti. Jos postilaatikko on johtajan päätelaitteessa, tulee päätelaitteen olla käytännössä jatkuvasti käynnissä, jotta postit reitittyvät ja saapuvat perille. Jatkuva käynnissä oleminen kuluttaa laitteen akkua. Varsinkin näyttö ja WLAN-radio kuluttavat virtaa suhteellisen paljon. Tämä aiheuttaa haasteen virtalähteiden lataamiselle taistelukentän olosuhteissa. Postilaatikko voi olla myös taistelijan reitittimessä, jolloin päätelaite voi olla virrattoman tai lepotilassa eikä se kuluta juurikaan virtaa. Postilaatikko ei itsessään kuluta virtaa, mutta MICS-palvelimen tulee löytää kansio, johon saapuva posti sijoitetaan. Jos postilaatikko on reitittimessä, se on MICS-palvelimen yhteydessä eikä WLAN-yhteyttä tarvita postien tai tilannetietojen välittämiseen enne kuin johtaja hakee postit palvelimelta päätelaitteelleen.

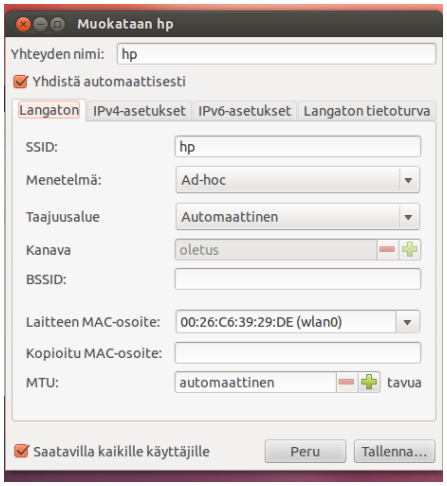
Haasteelliseksi jälkimmäinen ratkaisu muodostuu johtajan siirtyessä toisaalle. Johtajan tulisi ottaa reititin mukaansa ja reitittimeen pitäisi saada yhteys verkosta. Mukaan tulisi siis ottaa reititin ja radio. Kolmas vaihtoehto voisi olla reitittimeen liitettävä ulkoinen muisti esimerkiksi USB-tikku, jossa postilaatikon kansiot sijaitsisivat. Johtajan ollessa joukkonsa mukana tilannetiedot ja sähköpostit välittyisivät VHF-radiolla MICS-palvelimelta postilaatikkoon. Johtajan siirtyessä esimerkiksi ajoneuvoonsa hän voisi ottaa ulkoisen muistin mukaansa ja liittää sen joko päätelaitteeseensa tai ajoneuvon reitittimeen. Ratkaisu on esitetty kuvassa 12.



Kuva 12: Johtajan postilaatikon sijainti. Ylempänä johtaja on joukkonsa mukana, alempana johtaja on siirtynyt toiseen verkkoon.

Tapausta tutkittiin kenttäkokeilla. Kenttäkokeiden kuvaus ja raportointi ovat liitteessä 2.

Kenttäkokeiden perusteella voidaan todeta, että johtajan päätelaite voidaan liittää ajoneuvon langattomaan lähiverkkoon. Liittäminen voidaan tehdä joko AP- tai AdHoc-moodissa. Windows solmuilla käyttäjä joutuu AdHoc-verkkoa vaihtaessaan valitsemaan uuden verkon manuaalisesti, mutta verkon vaihtamiseen kuluva aika on alle kaksi sekuntia. Windows Vistassa AdHoc-verkko voidaan tallentaa myös liikkuva solmun verkonhallintatyökaluilla. Verkkoa vaihdettaessa uusi verkko tulee kuitenkin valita manuaalisesti ja suojausavain syöttää uudestaan, joten verkon tallennuksesta ei ole merkittävää hyötyä. Ominaisuus on poistunut Vistaa uudemmista Windows versioista. Ubuntu-solmulla voidaan siirtyä myös AdHoc-verkkojen välillä muuttamatta liikkuvan solmun asetuksia. Ubuntu säilyttää myös tallennetun verkon suojausavaimen. Siirtyminen vaatii aiemman verkon yhteyden katkeamisen. AP-moodissa sekä Windows- että Linux-käyttöjärjestelmissä voidaan verkko tallentaa järjestelmän omilla verkonhallintatyökaluilla. Ubuntun verkonhallintatyökalu verkon muokkausikkuna on esitetty kuvassa 13.

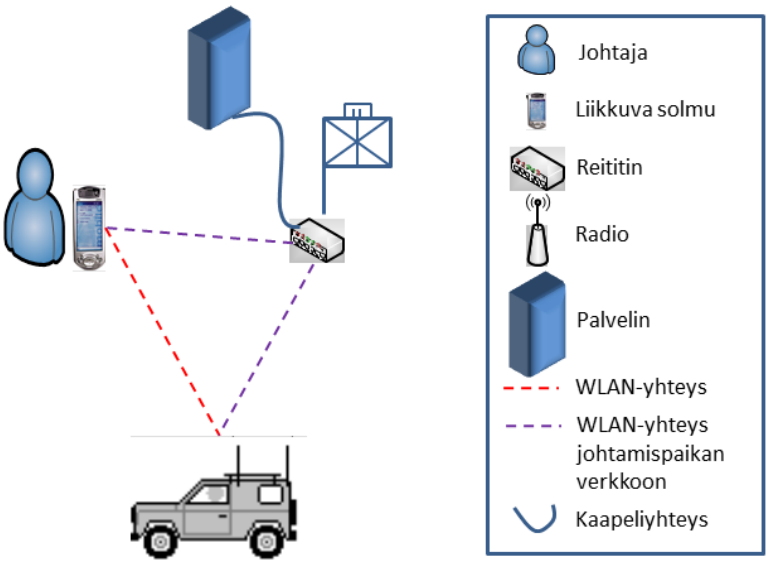


Kuva 13: Ubuntun verkonhallintatyökalun näkymä verkon muokkausikkunasta

Solmujen liikkuvuutta verkkojen välillä kuvataan kolmella siirtymistyypillä. Ensimmäinen tyyppi on siirtymätön (No-transition), jossa solmu ei siirry tai siirtyy samassa verkossa. BSS-siirtymisessä solmu siirtyy BSS-verkosta toiseen BSS-verkkoon saman ESS-verkon sisällä. ESS-siirtymisessä solmu siirtyy BSS-verkosta toisessa ESS-verkossa olevaan BSS-verkkoon. ESS-siirtymisessä standardi ei takaa ylemmän tason palveluiden säilyvyyttä.[12, s. 71] Haluttaessa varmistaa tiettyjen palveluiden säilyvyys tulisi siirtymisten siis tapahtua saman ESS-verkon alueella tai palveluiden säilyvyys tai käytettävyys tulee varmentaa.

4.3. Ajoneuvon WLAN laitteiston kaksinaisrooli

Tapauksessa johtaja päätelaitteineen saapuu ajoneuvolla johtamispaikalle. Ajoneuvossa on WLAN-radion sisältävä reititin ja johtamispaikalla on langaton lähiverkko. Ajoneuvon reitittimen tulisi pystyä liittymään johtamispaikan langattomaan lähiverkkoon. Edelleen johtajalla olevan päätelaitteen tulisi pysyä liittyneenä ajoneuvon reitittimeen WLAN-yhteyden välityksellä. Johtaja voi myös liittyä johtamispaikan langattomaan lähiverkkoon suoraan. Tapaus on esitetty kuvassa 14.



Kuva 14: Tapaus 3

Johtamispaikalla on palvelin tai johtamispaikan lähiverkko on liitetty verkkoon, jossa sijaitsee palvelin. Tavoitetilassa päätelaite pystyy päivittämään tietokantansa ajoneuvon reitittimen ja johtamispaikan langattoman lähiverkon kautta.

Tapausta tutkittiin kenttäkokeilla. Kenttäkokeissa luotiin koeympäristö, jossa langattomaan verkkoon jaettiin yksi ulkoyhteys. Ulkoyhteytenä käytettiin internetyhteyttä, joka saatiin todennettua OOKLA-nopeustestillä web-osoitteessa http://www.speedtest.net. Ulkoyhteys jaettiin WLAN-tukiasemalla tai matkapuhelimella. WLAN-yhteys sillattiin/toistettiin langattomalla toistimella. Toistin sijoitettiin lähelle solmuja, joilla mittaukset suoritettiin. Ennen mittauksia varmistettiin tulevan signaalin voimakkuus ja laatu solmujen omilla työkaluilla, jotta voitiin varmistua solmujen olevan yhteydessä nimenomaan toistimeen eikä tukiasemaan. Kaikissa tapauksissa suoritettiin kolme nopeustestiä jokaisella verkon solmulla, jotta yhteyden toimivuus ja vakaus saatiin varmistettua. Kenttäkokeiden kuvaus ja raportointi ovat liitteessä 2. Kenttäkokeessa suoritettujen mittausten tulokset ovat liitteessä 3.

Vaatimukset ajoneuvon reitittimen WLAN-ominaisuuksille:

- reitittimen on pystyttävä liittymään johtamispaikan langattomaan lähiverkkoon
  - 5 GHz taajuudella toimiva verkko
  - 2.4 GHz taajuudella toimiva verkko
- johtajan päätelaitteen on pysyttävä liittyneenä ajoneuvon reitittimen WLAN-radioon saavuttaessa toisen WLAN-verkon kantamalle
- johtajan päätelaitteen on saatava yhteys palvelimen tietokantoihin verkkojen välityksellä.

Kenttäkokeiden perusteella voidaan todeta, että johtajan liittyminen johtamispaikan langattomaan lähiverkkoon onnistuu aiemmissa tapauksissa kuvatuilla tavoilla riippuen verkon asetuksista ja ominaisuuksista. Haasteellisempi ja aiemmista tapauksista poikkeava tilanne on, jos johtaja liittyy omalla päätelaitteellaan ajoneuvon verkkoon ja ajoneuvoreititin edelleen johtamispaikan verkkoon.

Ajoneuvoreitin voi toimia toistimena tai siltana. Reititin voi toistaa eli kaiuttaa johtamispaikan verkon ajoneuvon sisälle. Ajoneuvon reititin voi liittyä johtamispaikan verkkoon ja jakaa ajoneuvoon toisen langattoman lähiverkon esimerkiksi tapauksessa, jossa johtamispaikan verkko on AP-moodissa ja ajoneuvoon halutaan AdHoc-verkko. Uusimpien standardien 802.11n ja 802.11ac mukainen MIMO-tukiaseman sisältävä reititin voi toimia yhtäaikaisesti kahdella taajuudella ja siihen voi liittyä sekä 2.4 GHz että 5 GHz taajuusalueilla toimivat solmut. MIMO-tekniikka tukee useita antenneja, jolloin ajoneuvon ulkopuolella voi olla antennit johtamispaikan verkkoon liittymistä varten ja ajoneuvon sisällä omaa lähiverkkoa varten. Johtamispaikan verkon jakaminen WDS-tekniikalla on mahdollista ja tällöin johtaja saa käyttöönsä johtamispaikan palvelimen palvelut ajoneuvon langattomassa verkossa. WDS-tekniikkaa ei kuitenkaan ole 802.11 standardeissa määritelty tarkasti ja toteutuksessa on valmistajakohtaisia eroja. WDS-moodia käytettäessä laitteet tulee testata jo hankintavaiheessa, jotta ne toimivat halutulla tavalla. Jos johtamispaikalla on käytössä 5 GHz:n verkko ja ajoneuvoon halutaan jakaa 2.4 GHz:n verkko, on varminta nykyisten standardien mukaisesti käyttää reititintä, jossa on omat WLAN-radiot molemmille verkoille.

4.4. Johtopäätökset

Ensimmäisessä tapauksessa yhteys voidaan toteuttaa sekä AP- että AdHoc-moodeissa. Verkon muodostavana solmuna kannattaa käyttää lähiradioon liitettyä taistelijanreititintä riippumatta käytössä olevasta moodista. Taistelijanreititin on pidettävä valmiustilassa MICS-palvelimen ja postilaatikon takia jatkuvasti. Taistelijanreitittimen virransyöttö on toteutettavissa radion akusta tai lisävirtalähteestä.

Toisessa tapauksessa siirtyminen verkosta toiseen onnistuu edelleen sekä AP- että AdHoc-moodeissa. Windows-päätelaitteilla AdHoc-verkosta toiseen siirtyminen vaatii asetusten manuaalista muuttamista. Mikäli toimitaan Windows-päätelaitteilla, kannattaa ajoneuvoreitittimessä käyttää AP-moodia.

Kolmannessa tapauksessa AP-moodi mahdollistaa ajoneuvon liittymisen johtamispaikan WLAN-verkkoon ja verkon edelleen jakamisen ajoneuvon sisälle. Käytettäessä kahta taajuutta yhtäaikaisesti verkkoon voi liittyä sekä 2.4 GHz että 5 GHz taajuutta käyttäviä solmuja. 5 GHz:n verkon jakaminen edelleen 2.4 GHz:n verkkona vaatii molemmille verkoille omat radionsa. Sekä AP- että AdHoc-moodeissa päätelaite voi siirtyä suoraan johtamispaikan verkkoon.

Taulukossa 2 on vertailtu infrastruktuuriverkon ja AdHoc-verkon vahvuuksia ja heikkouksia tapauksittain.

Tutkimustulosten perusteella voidaan tehdä tapauksista riippumattomia johtopäätöksiä. WLAN-verkon muodostamiseksi ja verkkoon liittymiseksi on suositeltavaa käyttää Linux-käyttöjärjestelmää kaikissa solmuissa.

Liitettäessä päätelaite staattisesti langattomaan lähiverkkoon ei käytettävällä verkkotyypillä tai moodilla ole merkitystä. Linux-koneen osalta on huomioitava AdHoc-verkkoon liityttäessä, että ip-asetukset on syötettävä ennalta. Verkkoasetukset voidaan tallentaa ja verkkoon liittyminen käy jatkossa automaattisesti. Windows kone kykenee hakemaan ip-osoitteen automaattisesti oletusasetuksilla, mutta suojattuun AdHoc-verkkoon liityttäessä on salausavain syötettävä aina.

Verkosta toiseen siirtyminen onnistuu AP-verkkojen välillä automaattisesti ja nopeasti, jos verkot on tallennettu päätelaitteeseen ja asetettu yhdistämään automaattisesti. AdHoc-verkoissa Windows-koneella pitää verkon vaihtaminen toteuttaa manuaalisesti. Myös suojausavain pitää syöttää käsin. Linuxin verkonhallintatyökalut mahdollistavat AdHoc-verkkojen asetusten tallentamisen myös liikkuvissa solmuissa. Tallennus koskee myös suojausavaimia.

Laajennettaessa verkkoa, tai jaettaessa verkon palveluita toiseen langattomaan lähiverkkoon tulee huomioida WDS-tekniikan standardoimattomuus. Eri laitevalmistajien laitteet eivät välttämättä toimi yhteen tai samalla tavalla. Käytettäessä kahta taajuutta yhtäaikaisesti verkkoon voi liittyä sekä 2.4 GHz:n että 5 GHz:n taajuutta käyttäviä solmuja, mutta 5 GHz:n verkon jakaminen edelleen 2.4 GHz:n verkkona tulee molemmille verkoille olla oma radio.

Taulukko 2: Infrastruktuuri- ja AdHoc-verkkojen vahvuudet ja heikkoudet tutkituissa tapauksissa

	Infrastruktuuriverkko		AdHoc-verkko	
	+	-	+	-
Tapaus 1	Verkko pysyy käytettävissä, kun tukiasema on päällä, vaikka päätelaite olisi välillä lepotilassa. Verkon salaus on toteutettavissa helposti.		Verkko muodostuu automaattisesti uudelleen päätelaitteiden määrän tai aktiivisuuden muuttuessa.	Windows-päätelaitteeseen tulee salausavain syöttää käsin liityttäessä salattuun verkkoon. Linux-päätelaitteeseen tulee syöttää ip-asetukset ennalta.
Tapaus 2	Päätelaitteeseen tallennetuilla verkoilla siirtyminen verkosta toiseen onnistuu nopeasti asetuksia muuttamatta.		Linux-päätelaitteilla verkon vaihtaminen onnistuu nopeasti ilman asetusten muuttamista.	Windows-päätelaitteilla verkkoon tulee liittyä manuaalisesti ja salausavaimet on syötettävä käsin.
Tapaus 3	Kahdella WLAN-radiolla varustettu tukiasema mahdollistaa 5 Ghz:n verkon palvelujen jakamisen 2.4 Ghz:n verkkoon.	WDS-tekniikan standardoimattomuus vaatii verkkoa laajennettaessa varmuuden laitteiden yhteensopivuudesta.	AdHoc-moodi mahdollistaa Linux-päätelaitteen liikkumisen verkosta toiseen.	Windows-päätelaiteilla tapauksen toteuttaminen AdHoc-moodissa vaatii asetusten muuttamista.

5. YHDISTELMÄ

5.1. Tutkimuksen tulosten arviointi

Tutkimuksen tuloksena voidaan todeta, että langattomia lähiverkkoja voidaan käyttää tiedonsiirtoon taistelukentän olosuhteissa. Langattomien lähiverkkojen käytettävyys ei rajaudu tutkittuihin tapauksiin. Lähdeaineiston ja kenttäkokeiden tulosten perusteella voidaan tehdä johtopäätöksiä myös erilaisiin tapauksiin ja käyttötarkoituksiin.

Toiminnalliset eli taktiset ja operatiiviset vaatimukset WLAN-perustaiselle tiedonsiirtojärjestelmälle on esitetty johtamisen näkökulmasta. Tiedonsiirtojärjestelmän tulee kyetä välittämään tilannetiedot riittävän tilannekuvan muodostamiseksi luotettavasti, eheänä, oikeaaikaisesti ja jatkuvasti. Verkkojen tulee mahdollistaa käyttäjän pääsy hänelle kuuluvaan tietoon.

Tarkat tekniset vaatimukset on kuvattu tapauskohtaisesti neljännessä luvussa. Päätelaitteiden tulee kyetä liittymään eri verkkoihin viiveettömästi ilman asetusten muuttamista. Verkon tiedonsiirtokapasiteetin tulee olla riittävä. Parhaiten näihin vaatimuksiin vastaavat Linux-pohjaiset solmut, jotka tukevat uusinta standardia.

Tutkimustulosten ja johtopäätösten luotettavuutta arvioitaessa esille nousevat validiteetti ja reliabiliteetti. Validiteetti tarkoittaa tulosten ja johtopäätösten pätevyyttä ja reliabiliteetti tulosten toistettavuutta. Tutkimuksen toisessa luvussa tutkittiin taistelukentällä tapahtunutta muutosta sekä suunnittelun ja johtamisen aiheuttamia vaatimuksia johtamisjärjestelmälle. Luvussa kuvatut muutokset ovat suurelta osin jo toteutuneet, joten niiden osalta johtopäätösten voidaan todeta olevan valideja. Luvun johtopäätöksinä esitetyt vaatimukset johtamisjärjestelmälle perustuvat Suomessa ja Yhdysvalloissa tehtyihin tutkimuksiin ja tutkijan näkemykseen tulosten sovellettavuudesta tutkimuksessa rajattuun johtamisjärjestelmään. Tulosten vastaavuus johtamisjärjestelmälle tulevaisuudessa asetettaviin vaatimuksiin on arvio ja vaatimuksia on tarkasteltava uudestaan viimeistään taistelun kuvan muuttuessa.

Luku kolme perustuu IEEE:n standardeihin ja standardoidusta tekniikasta tehtyihin julkaisuihin. Luvun tulokset ja johtopäätökset ovat valideja teoreettisella tasolla hyväksyttyjen standardien osalta. Laitevalmistajat rakentavat tuotteensa vastaamaan hyväksyttyjä standardeja, mutta tuotteissa saattaa olla ominaisuuksia, joita ei ole standardeilla määritetty tai ominaisuudet sisältyvät kehitteillä oleviin standardeihin. Luvussa esitetyt tulokset ja johtopäätökset eivät välttämättä vastaa kaikkia myytäviä tuotteita. Tulevista standardeista ja laitteiden sekä ominaisuuksien kehittymisestä ja aikatauluista tehdyt arviot perustuvat olemassa olevaan tietoon, standardointityöryhmien raportteihin ja laitevalmistajien mainoksiin, ja saattavat tarkentua tai jopa muuttua.

Luvussa neljä tutkitut tapaukset kuvaavat rajattuja tilanteita. Tapauksien johtopäätökset on tehty toisaalta standardeihin perustuvan tiedon pohjalta, toisaalta kenttäkokeen tuloksiin perustuen. Standardeihin perustuva tieto on validia jo edellä kuvatuista syistä. Kenttäkokeiden tulokset ovat rajatussa tutkimusympäristössä valideja kokeessa kuvatuilla laitteilla ja asetuksilla. Jotta tuloksista on saatu kattavat, on kokeet pyritty tekemään useammalla käyttöjärjestelmällä ja laitetyypillä. Kokeen tuloksissa on myös kerrottu, mikäli saatettaisiin saavuttaa poikkeava tulos käyttämällä toista laitetta, asetusta tai erillistä sovellusta.

Rakennettaessa langatonta verkkoa rajattuun käyttöympäristöön tulee järjestelmään hankittavat laitteet kokeilla suunnitelluilla asetuksilla, jotta voidaan varmistua laitteiden ja asetusten toimivuudesta halutulla tavalla.

Tutkimuksen reliabiliteettia arvioitaessa on arvioitava suoritettujen kokeiden ja toisaalta tutkimuksen johtopäätösten toistettavuus. Suoritetut kokeet on pyritty dokumentoimaan sellaisella tarkkuudella, että kokeet voidaan toistaa samantyyppisillä laitteilla asentamalla niihin samat käyttöjärjestelmät ja käyttämällä kuvattuja asetuksia. Tutkimuksen johtopäätökset on tehty kirjallisuustutkimuksen pohjalta varmentaen tutkimustulokset tapauskohtaisesti kenttäkokeilla. Tutkimuksen tulokset on toistettavissa tämän hetkisessä toimintaympäristössä. Vaatimusten muuttuminen ja tekniikan kehittyminen aiheuttavat tarpeen tulosten uudelleen arvioinnille.

5.2. Jatkotutkimustarpeet

Tutkimuksen johtopäätöksistä nousi runsaasti kysymyksiä ja ajatuksia jatkotutkimusten perustaksi. Yksityiskohtaista teknistä tutkimusta yksittäisten laitteiden ja asetusten käytettävyydestä tulee jatkaa, jos WLAN-yhteyksiä päädytään käyttämään taistelukentällä.

Tästä tutkimuksesta pois rajatut tietoturva ja autentikointi, sekä klusteroituneen verkon tai kahden AdHoc-verkon yhteenliittyminen ja uudelleen reititys ovat selvitettäviä asioita ennen kuin tekniikkaa voidaan laajamittaisesti ottaa käyttöön. Myös ulkopuolisten sovellusten eli apuohjelmien käyttö verkonhallinnassa tulisi selvittää.

WLAN-standardien kehitystä tulee seurata ja uusien standardien mukanaan tuomia ominaisuuksia tulee testata ja kokeilla käytännön sovelluksiin. Muitakin langattomia tiedonsiirtostandardeja on tutkittava ja selvitettävä niiden mahdollisuuksia tutkimuksen tapausten mukaisiin käyttötarkoituksiin.

Toisen tutkimustapauksen yhteydessä heräsi kysymys ajoneuvon muiden laitteiden ja radioverkkojen vaikutuksesta WLAN:n toimivuuteen ja WLAN:n vaikutuksesta ajoneuvokokonaisuuden toimivuuteen. Tällaisen kokonaisuuden osalta tutkimusta ei voida suunnata vain yhden spesifisen osa-alueen tutkimukseen vaan kokonaisuus on tutkittava kenttäkokeilla viimeistään kaikkien osakokonaisuuksien ratketessa.

Osa WLAN-verkkojen käytettävyyttä on niiden liittäminen laajempiin verkkoihin. Tässä tapauksessa kuvatut verkot ovat osa Maavoimien verkostokeskeistä tiedonsiirtojärjestelmän arkkitehtuuria ja liittyvät kiinteästi Maapuolustuksen viestijärjestelmä M18:an. Jatkotutkimus tulisi suunnata myös seuraavaan rajapintaan – WLAN-verkkojen liittämiseen M18-viestijärjestelmään. Nyt kuvatuissa tapauksissa reitittimet on liitetty M18-verkkoon VHF-radioilla ja tiedonsiirto tapahtuu MICS-palveluna.

Jatkossa MESH-tekniikan kehittyessä voitaneen AdHoc- ja AP-verkkojen väliset yhteydet toteuttaa joissain tapauksissa pitkän kantaman WLAN-yhteyksinä MESH-tekniikalla 802.16 Wimax, tai 802.11 standardeilla. Reitittimiin voidaan liittää HF, VHF ja UHF-radioiden lisäksi edellä kuvatun MESH-tekniikan mukaisia radioita, joilla kyetään TCP/IP-pohjaiseen tiedonsiirtoon. Ohjelmistoradio ja tulevaisuudessa kognitiivinen radio saattaa poistaa koko reititin/radio problematiikan. WLAN-verkossa on ulkoyhteyden tarjoavana solmuna kognitiivinen radio, joka valitsee parhaan yhteysvälin ja taajuusalueen WLAN-verkkojen väliselle liikenteelle.

LÄHTEET

[1] Alberts, D. & Hayes, R. *Planning: Complex Endeavors.* CCRP Publication series, USA, 2007. [Viitattu 14.1.2014] Saatavissa: http://www.dodccrp.org/html4/books_downloads.html.

[2] Alberts, D. & Hayes, R. *Understanding Command and Control.* CCRP Publication series, USA, 2003. [Viitattu 14.1.2014] Saatavissa: http://www.dodccrp.org/html4/books_downloads.html.

[3] ALSO Finland Oy. *ALSONet* [Verkkokauppa jälleenmyyjille]. [Viitattu 16.1.2014] Saatavissa: http://www.also.com/ec/cms3/fo/5710/start.jsp. (Vaatii jälleenmyyjän käyttäjätunnuksen.)

[4] Conner, W.S., Kruys, J., Kim, K. & Zuniga, J. *IEEE 802.11s Tutorial, Overview of the Amendment for Wireless Local Area Mesh Networking.* Dallas: 2006. [Viitattu 25.2.2014]. Saatavissa: http://www.ieee802.org/802_tutorials/06-November/802.11s_Tutorial_r5.pdf

[5] F9 Distribution Oy. *F9 verkkokauppa* [Verkkokauppa jälleenmyyjille]. [Viitattu 16.1.2014] Saatavissa: http://f9.fi. (Vaatii jälleenmyyjän käyttäjätunnuksen.)

[6] *Fresnel zone* [Wikipedia-sivu]. [Viitattu 24.1.2014]. Saatavissa: http://en.wikipedia.org/wiki/Fresnel_zone

[7] Heiskanen, M. Informaatiosodankäynti johtamissodankäynnin yläkäsitteenä. Kirjassa: Saarelainen, J., Tynkkynen, V., Aherto, J., Hyytiäinen, M. & Metteri, J. (toim.) Johtamissodankäynti, MPKK Taktiikan laitos, Julkaisusarja 2, Taktiikan asiatietoa n:o 2/2000. Helsinki: Edita Oy, 2000. s. 4-31. ISBN 951-25-1187-8.

[8] Hirsjärvi, S., Remes, P. & Sajavaara, P. *Tutki ja kirjoita.*10., osin uudistettu laitos. Jyväskylä: Gummerus Kirjapaino Oy, 2004. 436 s. ISBN 951-26-5113-0.

[9] Huttunen, M. *Monimutkainen taktiikka.* Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 1 Nro 2/2010. Helsinki: Edita Prima Oy, 2010. 329 s.

[10] *IEEE 802.11*. [Wikipedia-sivu]. [Viitattu 25.5.2014]. Saatavissa: http://en.wikipedia.org/wiki/IEEE_802.11

[11] *IEEE 802.11s*. [Wikipedia-sivu]. [Viitattu 25.5.2014]. Saatavissa: http://en.wikipedia.org/wiki/IEEE_802.11s

[12] IEEE standardi 802.11-2007 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[13] Iskanius, M. *Lukijalle.* Kirjassa: Saarelainen, J., Tynkkynen, V., Aherto, J., Hyytiäinen, M. & Metteri, J. (toim.) *Johtamissodankäynti, MPKK Taktiikan laitos, Julkaisusarja 2, Taktiikan asiatietoa n:0 2/2000.* Helsinki: Edita Oy, 2000. s. 1-3. ISBN 951-25-1187-8.

[14] Järvinen, P. *IT-tietosanakirja.* Jyväskylä: Tummavuoren Kirjapaino Oy, 2001. 815 s. ISBN 951-846-103-1

[15] Karsikas, J. *Maavoimien verkostokeskeisen tiedonsiirtojärjestelmä arkkitehtuuri ja sen toteuttaminen.* Diplomityö. Helsinki, 2007. Maanpuolustuskorkeakoulu, Tekniikan laitos. 153 s.

[16] Keane, M. *Dictionary of Modern Strategy and Tactics.* Maryland: Naval Institute Press Annapolis, 2005. 218 s. ISBN 1-59114-429-9

[17] Kuosmanen, P. Taktisten ad hoc-radioverkkojen toteuttamismahdollisuudet erilaisissa toimintaympäristöissä. Diplomityö. Julkaistu kirjana: Maanpuolustuskorkeakoulu, Tekniikan laitos, Julkaisusarja 1 No 20.Helsinki: Edita Prima Oy, 2004. 172 s. ISBN 951-25-1562-8.

[18] Kurssi- ja oppimateriaaliplone KOPPA (2010) [verkkojulkaisu]. Jyväskylän yliopisto, Humanistinen tiedekunta. [Viitattu 8.10.2013]. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/tapaustutkimus.

[19] Kuusisto, R. *Tilannekuvasta täsmäjohtamiseen, Johtamisen tietovirrat kriisin hallinnan verkostossa* [verkkojulkaisu]. Liikenne- ja viestintäministeriön julkaisuja 81/2005. ISBN 952-201-461-3. [Viitattu 3.3.2014]. Saatavissa: http://www.lvm.fi/fileserver/Julkaisuja 81_2005.pdf

[20] Libicki, M. *What is information warfare?* The Center for Advanced Consepts and Technology. National Defence University, 1995. 104.s

[21] Maavoimien esikunta. *Maapuolustuksen viestijärjestelmät M18.* Versio 0.9. 13.12.2013.

[22] Maavoimien yhtymän suunnittelun ja päätöksenteon perusteet B-osa (TLL IV Viranomaiskäyttö). Maavoimien esikunta, Mikkeli: 2010.

[23] McCann, S. & AshleyOfficial, A. *IEEE 802.11 working group project timelines - 2013-11-15.* Institute of Electrical and Electronics Engineers, Inc. (IEEE). [Viitattu

28.9.2013]. Saatavissa:
http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm#tgmb.

[24] Multitronic Oy. *Verkkokauppa.* [Viitattu 16.1.2014] Saatavissa: http://www.multitronic.fi.

[25] Nurmela, T. *Sotilaallisen kriisinhallintajoukon taistelutilaan vaikuttavat tekijät.* Esiupseerikurssin tutkielma. Julkaistu kirjana: Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2 Nro 1/2007. Helsinki: Edita Prima Oy, 2007. 91 s. ISBN 978-951-25-1823-4

[26] Oy Omnitele Ab: Puumalainen, J., Ojaniemi, A., Valtonen M. *Laajakaistatekniikoiden kehitys 2009 - 2015.* Liikenne- ja viestintäministeriön julkaisuja 46/2009. Helsinki, 2009. [Viitattu 16.1.2014] Saatavissa: https://www.lvm.fi/docs/fi/339549_DLFE-9557.pdf

[27] Pasivirta, P. *Teknisen kehityksen suuntalinjat*, Maanpuolustuskorkeakoulun Tekniikanlaitoksen Julkaisusarja 4, Tekniikan asiatietoa, n:o 1. Käännös FMV:n alkuperäistekstistä: Tekniska Utvecklingstrender. Helsinki: Edita Oyj, 2002. 216 s. ISBN 951-25-1338-2

[28] Peltomäki, J. *Kenttätelelääkinnän toteuttamisratkaisu.* Diplomityö. Helsinki, 2007. Maanpuolustuskorkeakoulu, Maasotalinja. 180 s.

[29] Pulkkinen, J. *WLAN 802.11n -standardin suorituskyky.* Insinöörityö. Helsinki, 2009. Metropolia ammattikorkeakoulu, Tietotekniikan koulutusohjelma. 39 s.

[30] Puska, M. *Lähiverkkojen tekniikka -Pro Training.* Jyväskylä: Gummerus Kirjapaino Oy, 2000. 348 s. ISBN 952-14-0373-x.

[31] Saaranen-Kauppinen, A. & Puusniekka, A. *KvaliMOTV - Menetelmäopetuksen tietovaranto* [verkkojulkaisu]. Tampere, 2006: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. [Viitattu 8.10.2013]. Saatavissa: http://www.fsd.uta.fi/menetelmaopetus/.

[32] Särkimäki, V. Lyhyen kantaman radiolähettimien soveltuvuus sähkökäyttöjen kunnon-

[33] Schiller, J. *Mobiili tietoliikenne*. Helsinki: Edita, 2001. 380 s. ISBN 951-826-216-0.

[34] *SSID*. [Wikipedia-sivu]. [Viitattu 24.1.2014]. Saatavissa: http://fi.wikipedia.org/wiki/SSID

[35] Suvanto, V. WLAN [Internet-artikkeli]. 2003. [Viitattu 23.1.2014] Saatavissa: http://muropaketti.com/artikkelit/sekalaiset/wlan

[36] Timonen, J. *A Dynamic Tactical Command System Operating with an Ad Hoc Network.* Diplomityö. Turku: 2011. Master of Science in Technology Thesis, University of Turku, Department of Information Technology, Software Engineering. 130 s.

valvonnan ja etädiagnostiikan tiedonsiirtotarpeisiin. Diplomityö. Lappeenranta: 2004. Lappeenrannan teknillinen yliopisto, Sähkötekniikan osasto. 79 s. [Viitattu 24.1.2014] Saatavissa: http://doria17-kk.lib.helsinki.fi/bitstream/handle/10024/34573/nbnfi-fe20051369.pdf?sequence=1

[37] Verkkokauppa.com Oyj. *Verkkokauppa*. [Viitattu 16.1.2014] Saatavissa: http://www.verkkokauppa.com/fi/catalog/10a/Verkko

[38] *WiFi Alliance* [Kotisivu]. 2014 [Viitattu 23.1.2014] Saatavissa: http://www.wi-fi.org/discover-wi-fi/wi-fi-direct

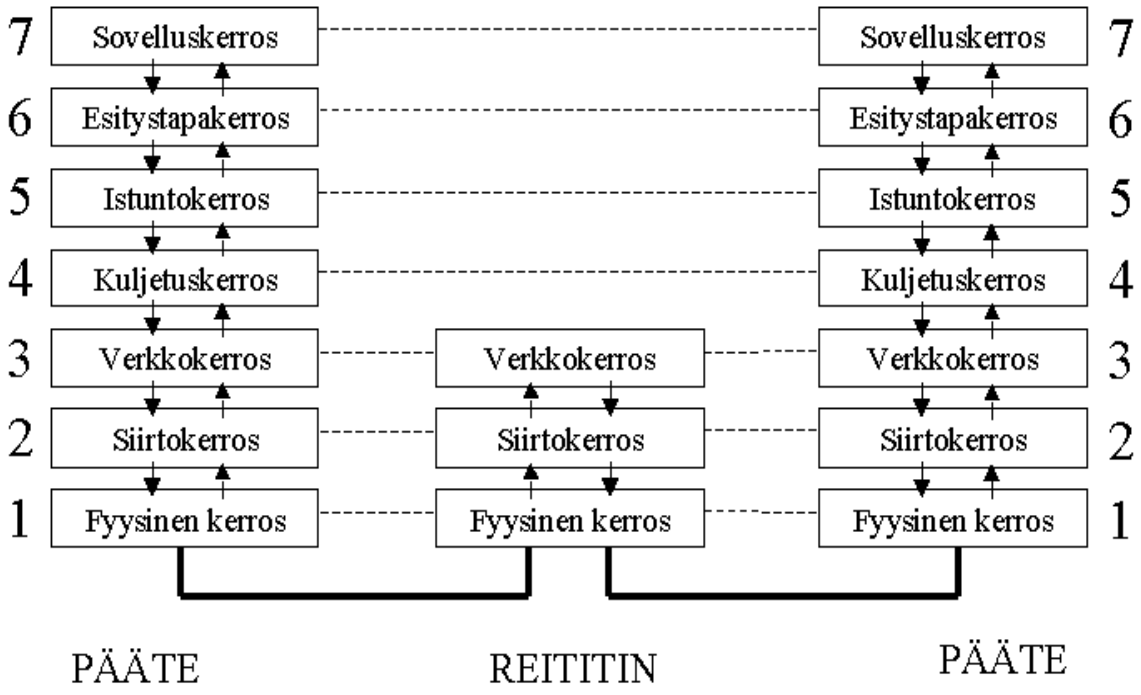
Liitteet

Liite 1 OSI-Malli

Liite 2 Kenttätutkimusraportti

Liite 3 Kenttäkokeen mittaukset 22.1.2014

OSI-malli


7
Sovelluskerros
Sovelluskerros
7
6
Esitystapakerros
Esitystapakerros
6
5
Istuntokerros
Istuntokerros
5
4
Kuljetuskerros
Kuljetuskerros
4
3
Verkkokerros
Verkkokerros
Verkkokerros
3
2
Siirtokerros
Siirtokerros
Siirtokerros
2
1
Fyysinen kerros
Fyysinen kerros
Fyysinen kerros
1
PÄÄTE
REITITIN
PÄÄTE

KENTTÄKOERAPORTTI

1. YLEISTÄ

Kenttäkoe toteutettiin kahdessa osassa 22.–23.1. ja 4.–5.3.2014. Kenttäkokeen ensimmäisessä vaiheessa 22.–23.1. tutkittiin WLAN-verkkojen ominaisuuksia ja toiminnallisuuksia myöhemmin kuvattavilla päätelaitteilla ja parametreilla. Päätelaitteiden käyttöjärjestelminä käytettiin Windows 7 ja Windows 8 -versioita sekä Android 4.1 ja Android 4.2 -käyttöjärjestelmiä Samsungin versioina. Kenttäkokeen toisessa vaiheessa 4.–5.3. laajennettiin kenttäkoetta tiettyjen alla tarkemmin kuvattujen ominaisuuksien osalta Linux Debian 7.4 ja Windows Vista -käyttöjärjestelmillä varustetuilla päätelaitteilla.

1.1. Tavoite

Kenttäkokeen tavoitteena oli selvittää rajattujen parametrien ja moodien tekninen käytettävyys. Kenttäkokeen tulosten perusteella on tehty johtopäätöksiä parametrien ja moodien käytettävyydestä tutkimuksen rajatuissa tapauksissa ja toisaalta pyritty myös tekemään yleistyksiä vertaamalla tutkimustuloksia lähdemateriaaliin.

1.2. Kenttäkokeen tutkimuskysymykset

- Voiko yksittäinen päätelaite liikkua AdHoc -verkosta toiseen?
- Mitkä ovat käyttöjärjestelmien erot AdHoc -verkoissa liikuttaessa?
- Voiko AdHoc -verkkoa laajentaa toistimella?
- Voiko Infrastuktuuriverkkoa laajentaa toistimella?
- Saadaanko ulkoyhteys jaettua toistettuun verkkoon AP ja AP + WDS moodeissa?

1.3. Toteutus

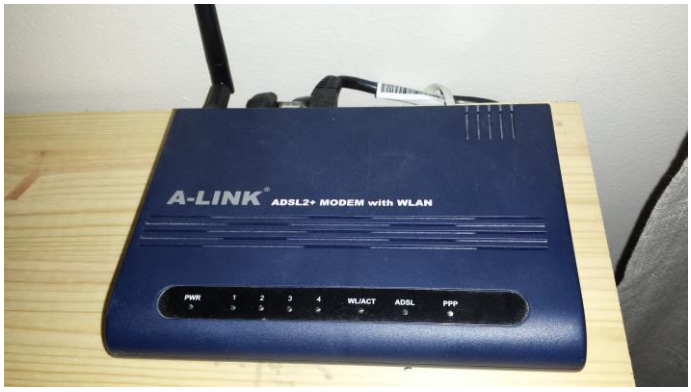
1.3.1 Tutkimusympäristö

Kenttäkokeen molemmat vaiheet toteutettiin tutkijan kotitoimistossa. Ulkoyhteytenä käytettiin ADSL-yhteyttä, jonka teoreettinen nopeus on 8/1 Mbit. Tutkimuksessa ei tutkittu verkkojen kantamaa eikä yhteysetäisyyksien vaikutusta verkkojen siirtonopeuksiin, joten tutkimusympäristö pienet etäisyydet eivät vaikuta tutkimustuloksiin. Eri verkkojen välillä siirtymistä tutkittaessa solmut, joihin liityttiin, sijaitsivat kuitenkin omakotitalon eri huoneissa, jotta voitiin signaalin voimakkuuteen perustuen todeta siirtymisen verkosta toiseen tapahtuneen myös tapauksissa, joissa verkko oli sillattu ja tukiasemat käyttivät samaa SSID:tä. Tutkimusympäristönä käytetyssä tilassa kuuluivat myös kaksi erillistä AP-moodissa olevaa langatonta lähiverkkoa kanavilla 7 ja 11. Nämä verkot eivät liittyneet kenttäkokeeseen eikä niitä ole huomioitu muuten kuin valitsemalla AP-moodia tutkittaessa tukiasemaan kanava, jota nämä ulkopuoliset verkot eivät häiritse.

1.3.2 Kenttäkokeessa käytetyt tukiasemat ja päätelaitteet

Ulkoyhteys jaettiin kenttäkokeissa A-LINK RR24AP tukiasemalla. Kyseessä on yhdistetty ADSL 2/2+ modeemi, reititin ja WLAN tukiasema. Tukiasema on esitetty kuvassa 14.

WLAN-yhteyden laajentamiseen käytettiin ZyXEL WRE2205 toistinta, jolla testattiin sekä AP-verkon että AdHoc-verkon laajentamista. Toistin on esitetty kuvassa 15.



Kuva 15: ADSL-modeemina ja WLAN-tukiasemana käytetty A-LINK RR24AP

Kuva 16: Verkon laajentamiseen käytetty ZyXEL WRE2205

Päätelaitteina testissä käytettiin neljää kannettavaa tietokonetta, yhtä matkapuhelinta ja yhtä tablettia sekä yhtä pöytä-työasemaa. Kannettavat tietokoneet olivat Lenovo ThinkPad Edge E325 – Windows 7 Professional käyttöjärjestelmällä, HP EliteBook 8560p – Windows 7 Enterprise, HP Pavilion 15-b155so SleekBook – Windows 8 sekä Lenovo T400 – Linux. Kokeissa käytetty matkapuhelin oli Samsung S4:ä ja tablettina Samsung Note 10.1. Pöytä-työaseman kokoonpanon kuvaaminen ei ole tutkimuksen tuloksen kannalta merkityksellinen. Kyseinen tietokone ei ole tunnetun valmistajan myyntimalli vaan tutkijan itse komponenteista kokoama perus kotikäyttötasoinen muutaman vuoden ikäinen työasema. Käyttöjärjestelmänä pöytä-työasemassa on Windows Vista Home Premium. Päätelaitteet on esitetty kuvissa 17–22.

Kuva 17: Lenovo Edge E325

Kuva 18: Lenovo T400

Kuva 19: HP EliteBook 8560p

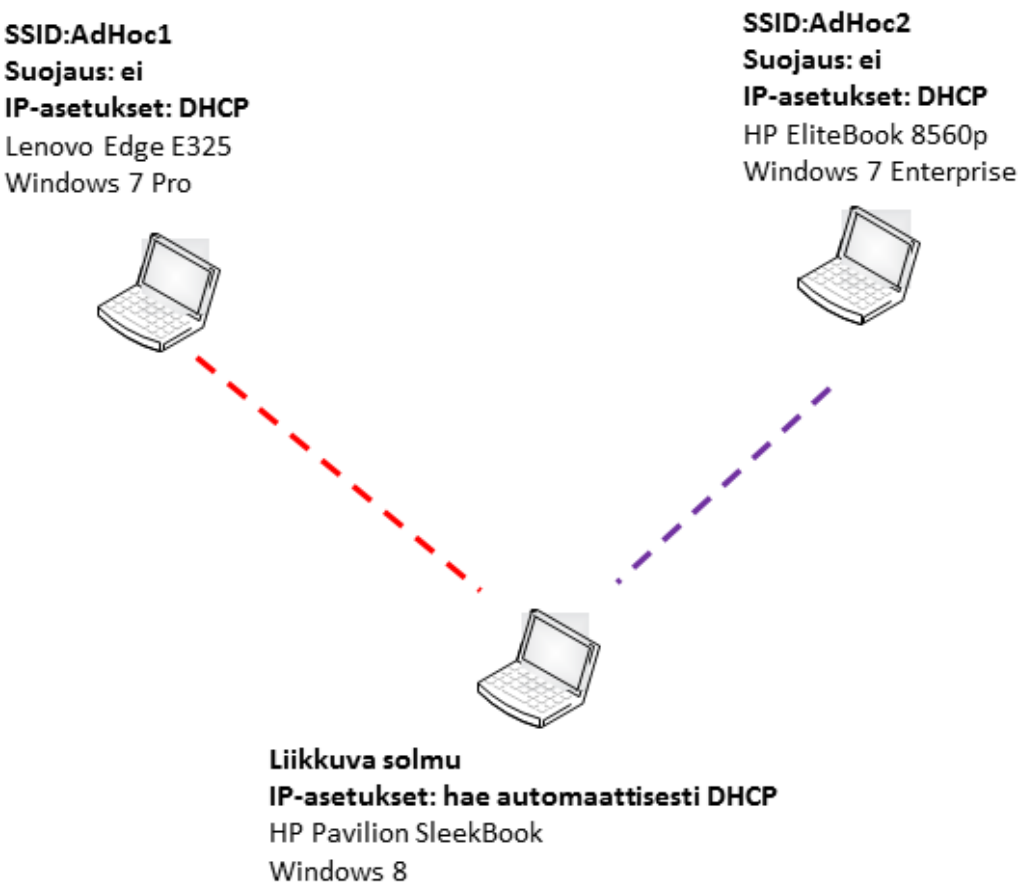
Kuva 20: HP Pavilion 15-b155so SleekBook [Kuvan lähde:Sunlogix tukkumyynti http://www.sunlogix.fi]

Kuva 21: Samsung S4

Kuva 22: Samsung Note 10.1

1.3.3 Koe 1 – siirtyminen AdHoc-verkosta toiseen

Ensimmäisessä kokeessa luotiin kaksi AdHoc-verkkoa, joihin liitettiin kolmas solmu. Kolmas solmu liikkui AdHoc-verkosta toiseen. Ensimmäinen AdHoc-verkko luotiin Lenovo ThinkPad Edge E325 kannettavalla tietokoneella ja toinen verkko HP EliteBook 8560p kannettavalla tietokoneella. Liikkuvana solmuna käytettiin HP Pavilion 15-b155so SleekBook kannettavaa tietokonetta. AdHoc verkot luoneissa koneissa oli käyttöjärjestelmänä Windows 7. Liikkuvan solmun käyttöjärjestelmänä oli Windows 8. Kokeen kokoonpano ja tärkeimmät asetukset on esitetty kuvassa 22.

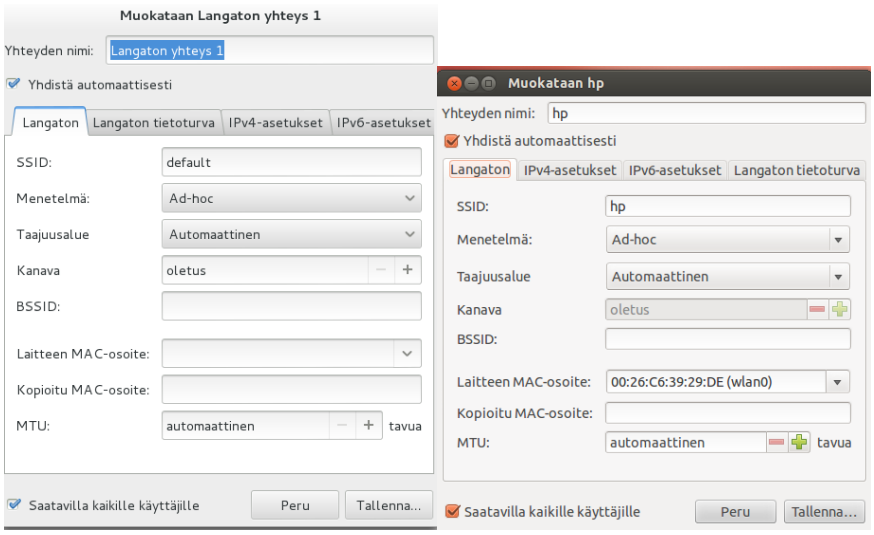


Kuva 23: Kokeen 1 kokoonpano ja tärkeimmät asetukset kenttäkokeen ensimmäisessä vaiheessa,

Koejärjestelyjä luotaessa havaittiin, että Windows 8 -käyttöjärjestelmän verkonhallintatyökalut eivät mahdollista AdHoc-verkon luomista. Windows 7 -koneilla verkon luominen on helppoa, mutta saman nimisiä AdHoc verkkoja ei pysty luomaan kuuluvuusalueen sisälle. Windows 7 ja 8 -koneiden verkonhallintatyökalut eivät mahdollista AdHoc-verkon tallentamista muissa kuin verkon luovassa koneessa. AdHoc-verkosta toiseen siirtyminen vaatii Windows 7 ja 8 -koneissa aina käyttäjältä verkon valitsemisen. Automaattinen AdHoc-verkkoon liittyminen ei ole mahdollista Windows 7:n ja 8:n verkonhallintatyökaluilla. AdHoc-verkon luominen Windows 8 -koneissa on mahdollista erillisillä apuohjelmilla, kuten Winhoc.

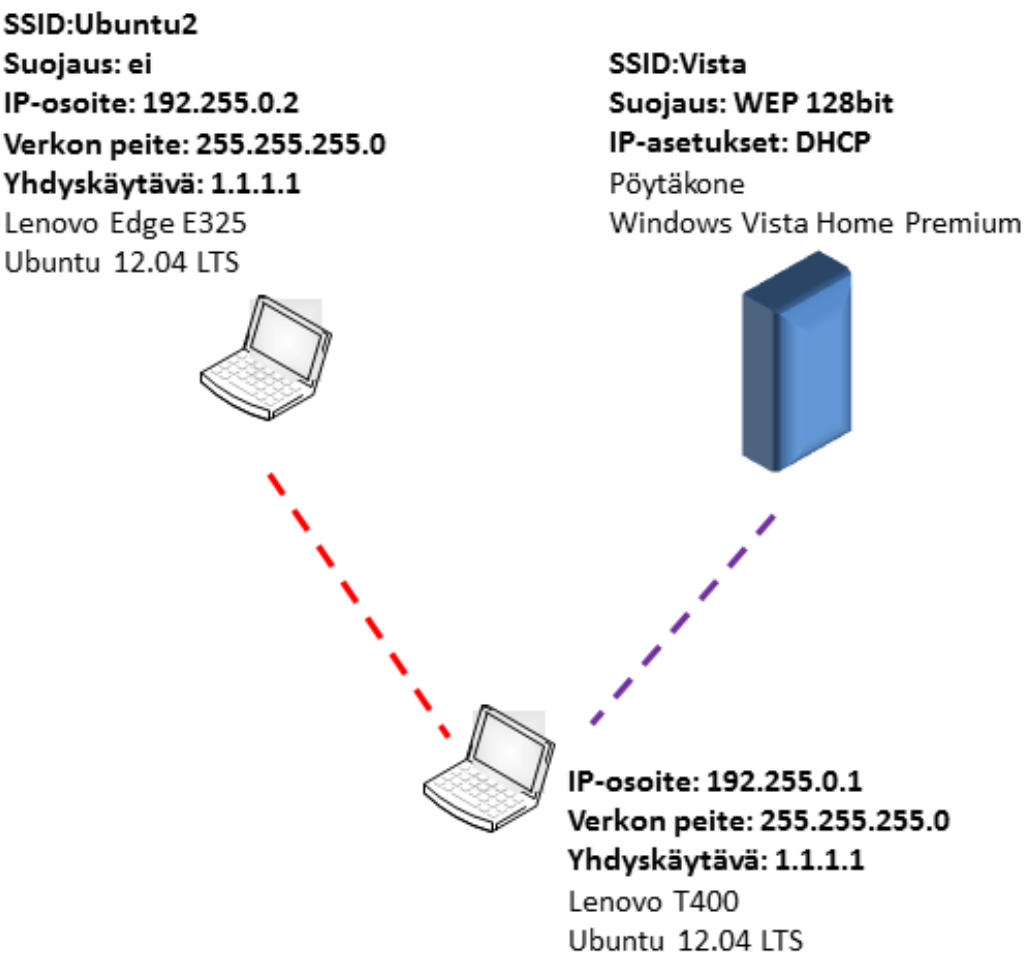
AdHoc-verkosta toiseen siirtyminen onnistui kokeessa käytetyllä HP SleekBook kannettavalla alle kahdessa sekunnissa salaamattomassa verkossa. Mikäli verkossa käytetään salausta, verkon vaihtaminen hidastuu, koska verkkoa eikä näin ollen salausavaintakaan ole tallennettuna koneen muistiin. Salausavain täytyy syöttää jokaisessa verkon vaihdossa, vaikka salauksena käytettäisiin samaa salausta samalla salausavaimella. Salaamaton verkko mahdollistaa kaikkien alueella olevien WLAN-päätelaitteiden liittymisen verkkoon. AdHoc-verkon rakentuessa jatkuvasti päätelaitteiden liittyessä verkkoon ja erotessa siitä on verkon valvonta vaikeaa ja ylimääräinen verkon jäsen voi jäädä huomaamatta.

Koetta jatkettiin 4.3.2014 selvittämällä mahdollistavatko Windows Vista ja Linux Ad-Hoc-verkon tallentamisen ja automaattisen uudelleen yhdistämisen. Vista-koneena käytettiin pöytätyöasemaa. Lenovo T400 -kannettavaan tietokoneeseen asennettiin käyttöjärjestelmäksi Debian 7.4. Käyttöjärjestelmän ydin on niin vanha, ettei se tunnistanut T400:n Intel WLAN-verkkokorttia. Tutkija asensi kannettavaan Intelin ajurin kyseiselle verkkokortille. Debian ei kuitenkaan tunnistanut verkkokorttia ja rajoitetusta tutkimusajasta johtuen koneeseen asennettiin Debianin arkkitehtuurin pohjalta rakennetun Ubuntun versio 12.04 LTS. Debianin ja Ubuntun verkonhallinta työkalut ovat ulkoisesti identtiset ja käyttöjärjestelmien vahvasta sukulaisuudesta johtuen voidaan Ubuntulla tehtyjen kokeiden todeta vastaavan Debianin ominaisuuksia riittävällä tarkkuudella. Verkonhallinta työkalut on esitetty kuvassa 23.



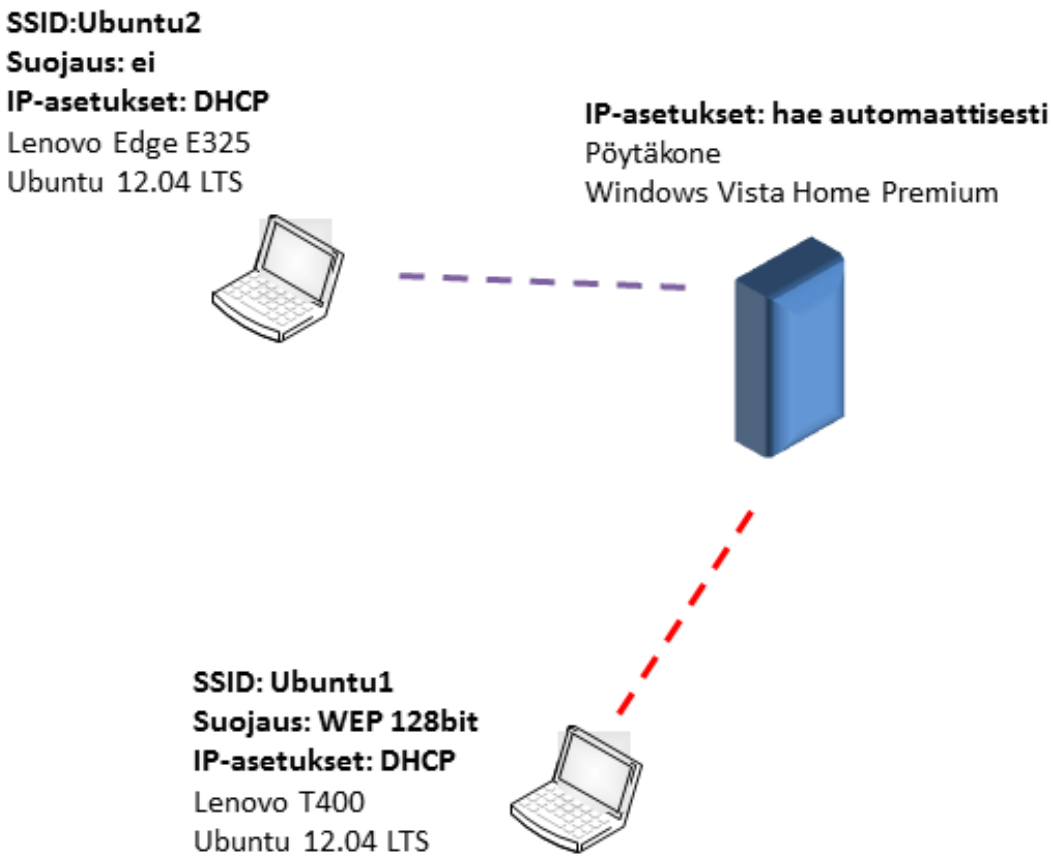
Kuva 24: Linuxin verkonhallintatyökalun verkon muokkausikkuna. Vasemmalla Debian, oikealla Ubuntu.

Windows-käyttöjärjestelmien verkonhallinta ei mahdollista AdHoc-verkon tallentamista ja automaattista verkkoon yhdistämistä myöskään Vistan verkonhallintatyökaluilla. Vistassa on mahdollista tallentaa verkko, mutta yhteyden katketessa yhteys täytyy muodostaa manuaalisesti. Mikäli AdHoc-verkkoon asennetaan suojaus, tulee myös suojausavain syöttää joka kerta muodostettaessa yhteys, vaikka verkko olisi tallennettu. Linux-koneen muodostamaan Ad-Hoc-verkkoon liittyminen onnistuu Windows-työasemalla kivuttomasti. Myös kahden Ubuntu-koneen välillä todettiin sama havainto kuin edellä Linux – Windows yhteydessä. Ubuntu-kone ei pystynyt liittymään Ubuntu-koneen luomaan AdHoc-verkkoon. Kokeen kokoonpano ja tärkeimmät asetukset on esitetty kuvissa 25–27.



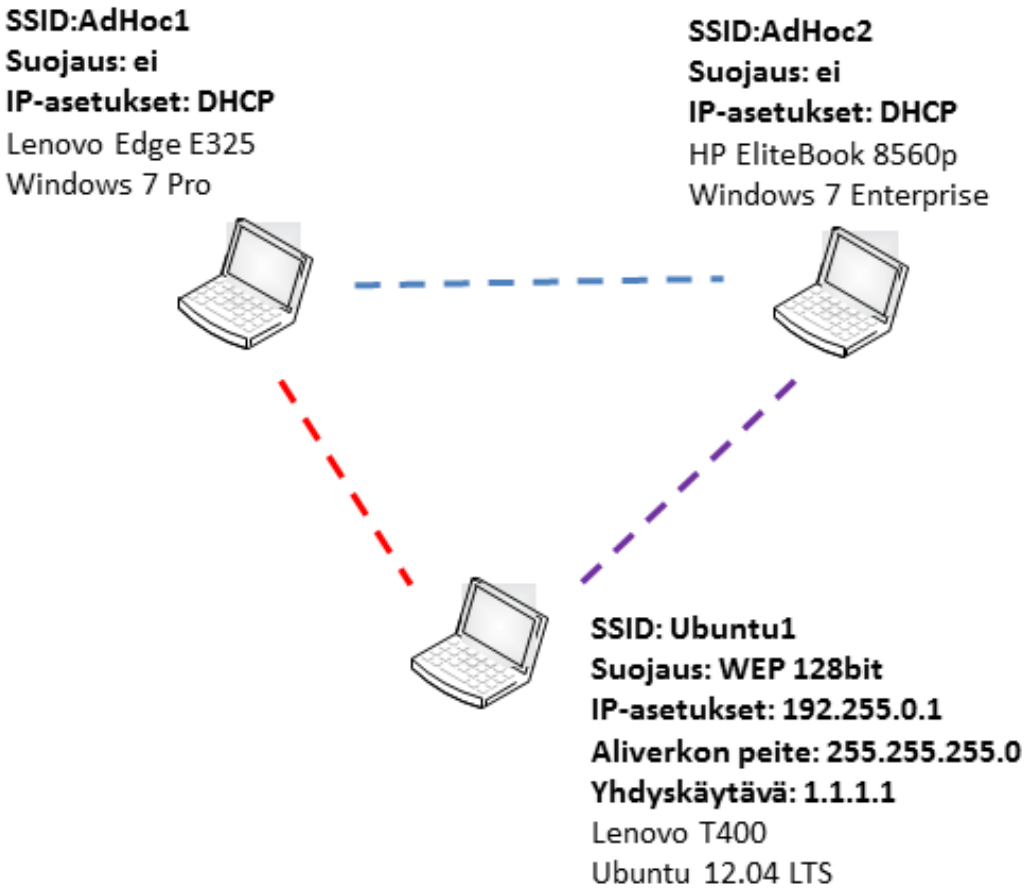
Kuva 25: Kokeen 1 kokoonpano ja tärkeimmät asetukset kenttäkokeen toisessa vaiheessa. Verkko luotiin Ubuntu-koneella.

Linux-työasema tunnistaa Windows-koneen muodostaman AdHoc-verkon, muttei pysty liittymään siihen automaattisesti. Tämän havainnon jälkeen myös Lenovo Edge E325 -kannettavaan tietokoneeseen asennettiin Ubuntu, jotta voidaan kokeilla AdHoc-verkkoon liittyminen kahden Linux-järjestelmän välillä.



Kuva 26: Kokeen 1 kokoonpano ja tärkeimmät asetukset kenttäkokeen toisessa vaiheessa. Verkko luotiin Vista-koneella.

Asettamalla verkon asetuksista ip-osoite, aliverkon peite ja oletusyhdyskäytävä saatiin Ubuntu-kone liittymään luotuun AdHoc-verkkoon. Ubuntun virallinen dokumentaatio verkko-osoitteessa https://help.ubuntu.com ohjeistaa AdHoc-verkon luomisen ja verkkoon liittymisen yhteydessä määrittämään IPv4-asetukset manuaalisesti. Oletusasetuksilla Ubuntu määrittää AdHoc-verkon asetuksissa jakavansa verkkoa toisille solmuille. Ulkoyhteyden jakaminen onnistuu oletusasetuksilla, mutta solmu ei pysty liittymään toisten luomiin AdHoc-verkkoihin. Kun asetukset oli määritetty manuaalisesti, liittyi Ubuntu-kannettava sekä toisen Ubuntu-kannettavan että Windows-kannettavan luomiin AdHoc-verkkoihin. Ubuntu mahdollistaa AdHoc-yhteyden tallentamisen myös asiakassolmuun. Tallentamalla Ubuntuun kahden AdHoc-verkon asetukset liittyi Ubuntu-kannettava automaattisesti toiseen AdHoc-verkkoon ensimmäisen yhteyden katkettua. Tutkija ei kuitenkaan löytänyt Ubuntun verkonhallintatyökaluista mahdollisuutta priorisoida verkkoja. Verkon vaihto tapahtui joko manuaalisesti, tai olemassa olevan yhteyden katkettua.

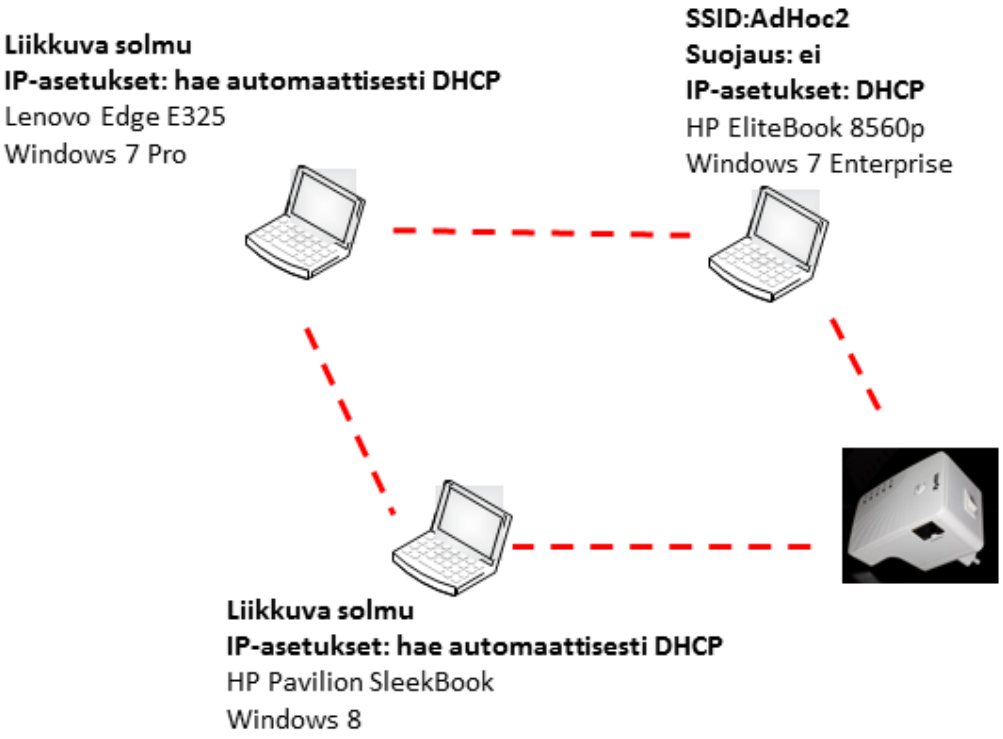


Kuva 27: Kokeen 1 kokoonpano ja tärkeimmät asetukset kenttäkokeen toisessa vaiheessa. Ubuntu-koneisiin on asetettu IP-asetukset manuaalisesti.

AdHoc-verkkoon yritettiin liittyä myös Android 4 päätelaitteilla. Android ei tue oletuksena AdHoc-verkkoja. Android käyttöjärjestelmässä on WiFi Direct toiminnallisuus. Android päätelaitteilla 802.11-standardien mukaiseen AdHoc-verkkoon liittyminen vaatii erillisen apuohjelman käyttämistä.

1.3.4 Koe 2 – AdHoc verkon laajentaminen toistimella

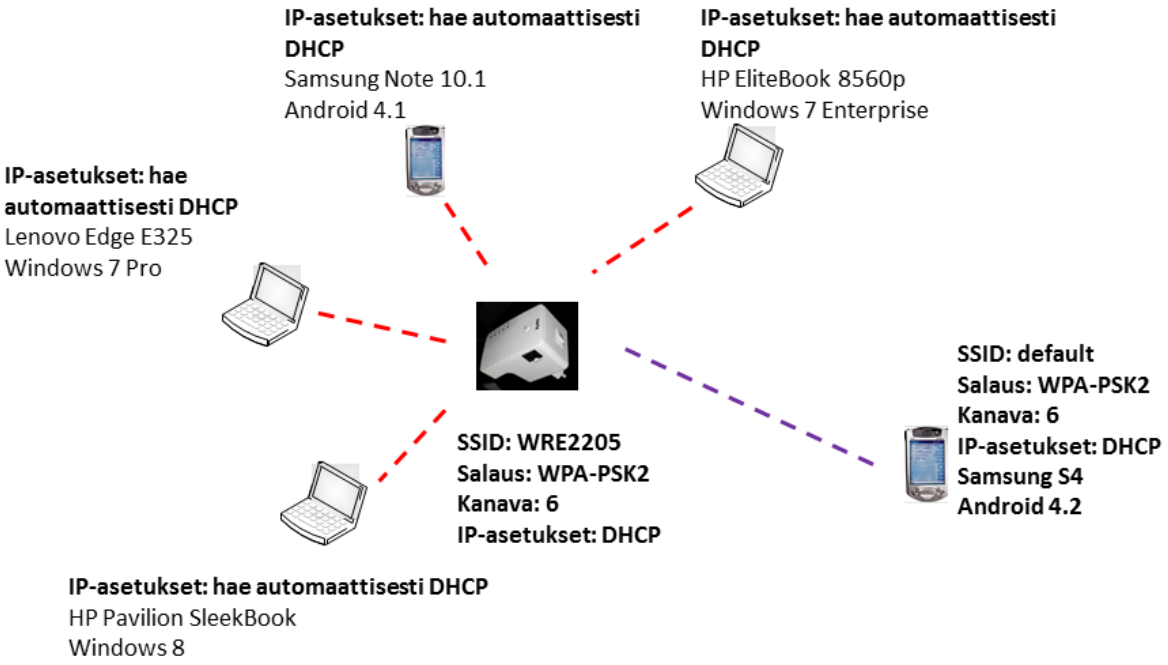
AdHoc verkon laajentamista yritettiin ZyXEL WRE2205 toistimella. Kokeessa toistin tunnisti AdHoc-verkon, mutta ei kyennyt liittymään siihen eikä toistamaan verkkoa. Kokeen kokoonpano ja tärkeimmät asetukset on esitetty kuvassa 28.



Kuva 28: Kokeen 2 kokoonpano ja tärkeimmät asetukset.

1.3.5 Koe 3 – infrastruktuuriverkon laajentaminen

Kolmannessa kokeessa jaettiin HSDPA+-tasoista mobiiliyhteyttä asettamalla Samsung S4 puhelimen WLAN-radio tukiasemaksi. S4 oli mittaushetkellä noin kahden kilometrin päässä tukiasemasta. Toistimena käytettiin ZyXEL WRE2205-toistinta. Toistin on 802.11n-standardin mukainen. Toistin tunnisti S4:n jakaman verkon b/g/n standardeja tukevaksi verkoksi. Toistin pyrki jakamaan oletusarvoisesti verkon alkuperäisellä SSID:llä käyttäen samaa kanavaa ja salausta. Käytössä oli kanava 6. Samassa huoneessa oli kokeessa neljä käytetty langaton lähiverkko kanavalla 1. Tilaan kuuluivat myös kaksi muuta langatonta lähiverkkoa kanavilla 7 ja 11. Käytetty salaus oli WPA PSK2. Verkon toimivuus testattiin vaihtamalla toistimen jakaman verkon SSID, jotta voitiin varmistua solmujen olevan liittyneenä toistimen jakamaan verkkoon. Toistin ei mahdollistanut taajuuden valintaa 2.4 GHz ja 5 Ghz välillä. Toistin jakoi verkon 802.11n standardin mukaisena. Kokeen kokoonpano ja tärkeimmät asetukset on esitetty kuvassa 29.

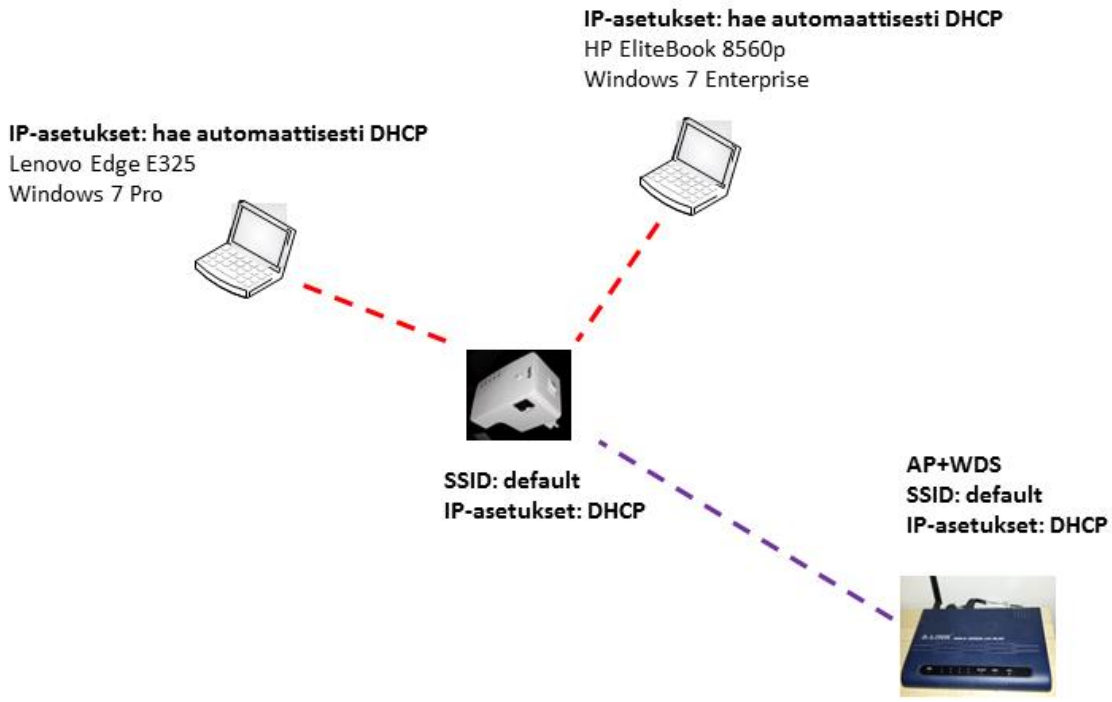


Kuva 29: Kokeen 3 kokoonpano ja tärkeimmät asetukset.

Verkkoon liittyneet solmut näkevät toisensa, mutta internetyhteys on vain yhden solmun käytössä. Verkkoon liitetty Samsung Note 10.1 -tabletti sai toistimen jakaman internetyhteyden ilman ongelmia. Samsung Notella suoritettujen yhteyden nopeustestien latausnopeudet (download) olivat 6.2 Mbit/s ja 8.6 Mbit/s välillä. Hitain lähetysnopeus (upload) oli 0,6 Mbit/s ja nopein 2,4 Mbit/s. Arvot eivät itsenäisinä kerro toistetun verkon toimivuudesta kuin, että toistin kykenee jakamaan ulkoyhteyttä yli 6 Mbit/s nopeudella. Verrattaessa arvoja Samsung S4:n jakaman yhteyden nopeuteen voidaan tehdä johtopäätöksiä toistimen aiheuttamista häviöistä lähiverkon nopeuteen. S4:n mobiiliyhteyden latausnopeus oli mittaushetkellä kolmessa mittauksessa välillä 9,4–9,8Mbit/s. Lähetysnopeus oli kaikissa kolmessa mittauksessa 1,6 Mbit/s. Latausnopeudessa Noten saamat tulokset ovat 10–30% heikompia verrattuna S4:n yhteyksiin. Tässä tapauksessa voidaan arvioida toistetun yhteyden olevan hitaampi kuin alkuperäinen latausnopeus. Lähetysnopeus oli Notella kahdessa mittauksessa kolmesta nopeampi kuin S4:n mobiiliyhteyden mitattu lähetysnopeus. Suurella todennäköisyydellä sekä latausnopeuksien että lähetysnopeuksien erot johtuvat mobiiliyhteyden epästabiiliudesta. Yhteysnopeudet vaihtelevat suuresti varsinkin kuuluvuusalueen reunoilla.

1.3.6 Koe 4 – infrastuktuuriverkon laajentaminen WDS-moodissa

Toisessa kokeessa jaettiin ADSL-yhteyttä A-LINK RR24AP -tukiasemalla. Kyseessä on yhdistetty ADSL 2/2+ modeemi, reititin ja WLAN-tukiasema. Tukiasema jakoi WLAN-yhteyden kanavalla yksi. Yhteys oli salaamaton. Tukiasema asetettiin AP + WDS -moodiin. Asetuksella pyrittiin tilanteeseen, jossa tukiaseman ja sillan välille muodostuu linkki ja molemmat laitteet tarjoavat langattoman verkon kuuluvuusalueellaan. Solmuina käytettiin Lenovo Thinkpad Edge E325 sekä HP EliteBook 8560p kannettavia tietokoneita. Nopeuksien vertailua varten yhteysnopeus mitattiin myös ethernetliitynnällä reitittimeen kytketyllä työasemalla. Lenovon latausnopeudet olivat välillä 5,7–5,9 Mbit/s, HP:n 6,3–7,2 Mbit/s ja ethernet-liityntäisen työaseman latausnopeus oli kaikissa kolmessa mittauksessa 7,1 Mbit/s. Lähetysnopeudet olivat Lenovolla 0,9 Mbit/s, HP:lla 0,8–0,9 Mbit/s ja ethernet-liityntäisellä työasemalla 0,9 Mbit/s. Kokeen kokoonpano ja tärkeimmät asetukset on esitetty kuvassa 30. Valmistajan skenaario infrastuktuuriverkon laajentamisesta on esitetty kuvassa 31.



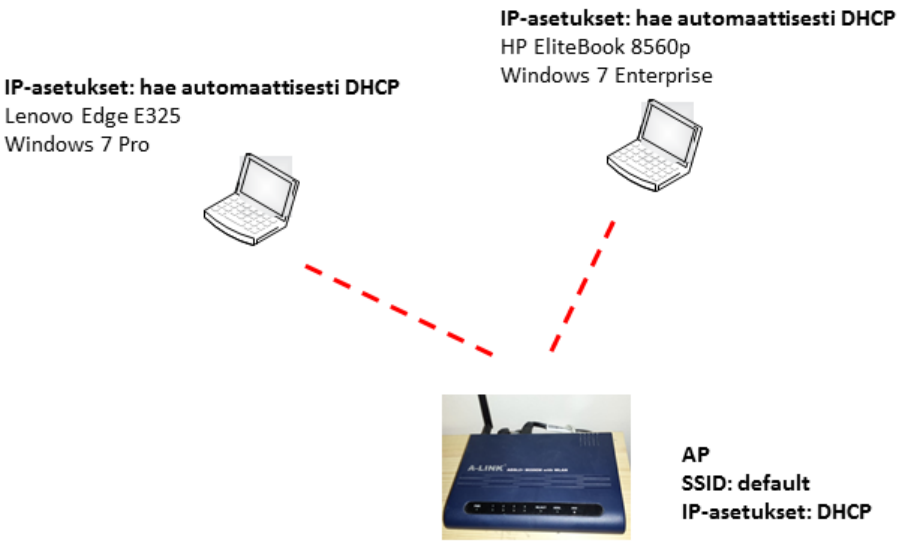
Kuva 30: Kokeen 4 kokoonpano ja tärkeimmät asetukset.

Kuva 31: Infrastruktuuriverkon laajentaminen valmistajan skenaarion mukaisesti [lähde: http://www.zyxel.com/fi/fi/products_services/wre2205.shtml?t=p]

Johtopäätöksenä voidaan todeta latausnopeuden olleen langattomassa verkossa 10–20% hitaamman kuin ethernet-verkossa. Lähetysnopeus oli kaikilla laitteilla sadan kilobitin vaihteluvälin sisällä. Kymmenen prosentin, eli noin sadan kilobitin eroa lähetysnopeudessa ei voi laskea merkitykselliseksi tämän mittauksen perusteella, koska yhteysnopeuksien vaihtelu latausnopeuksissa samalla solmulla oli jopa megabitin suuruinen.

1.3.7 Koe 5 – sillan / toistimen aiheuttama nopeushäviö

Viidennellä kokeella selvitettiin aiheuttaako toistin nopeushäviötä. Neljäs koe toistettiin samoilla tukiaseman asetuksilla ilman toistinta. Solmuna käytettiin HP EliteBook 8560p kannettavaa tietokonetta. Kokeen tulokset ovat identtiset, korkeintaan 10 kbit/s nopeusvaihteluilla. Samanlaisia vaihteluita havaittiin sekä toistimella että ilman toistinta suoritetussa kokeessa. Kokeen kokoonpano ja tärkeimmät asetukset on esitetty kuvassa 31.



Kuva 32: Kokeen 5 kokoonpano ja tärkeimmät asetukset.

1.3.8 Koe 6 – Infrastruktuuriverkon laajentaminen AP-moodissa

Kuudes koe toteutettiin samoilla laitteilla kuin neljäs koe. Poikkeuksena tukiasema asetettiin AP-moodiin ilman WDS:ia. Verkkoon pääsi kaikki testin laitteet, mutta toistin ei kyennyt jakamaan internetyhteyttä kuin yhdelle solmulle kerrallaan.

Kapteeni Mikko Rasimuksen tutkielman LIITE 3

Kenttäkokeen mittaukset 22.1.2014							
	Laite	Kanava	download Mbit/s	upload Mbit/s			
Koe 4							
Lähettävä WLAN tukiasema	Samsung S4	Channel 6	9,38	1,58			
WPA PSK2	b/g/n		9,74	1,59			
			9,78	1,6			
Repeater	Zyxel WRE2205						
Solmu	Samsung Note 10.1		6,77	0,58			
			8,57	2,32			
			6,23	2,41			
Koe 5							
Lähettävä WLAN tukiasema	A-link RR24AP ADSL 2/2+ modem	Channel 1	Verkossa 7 päätelaitetta, joista 5 WLAN:n välityksellä. Kaksi s				
ei salausta	b/g						
	AP/WDS						
Repeater	Zyxel WRE2205						
Solmu	Lenovo TfhinkPad Edge E325		5,7	0,9			
			5,9	0,91			
			5,83	0,91			
	HP Elitebook 8560p		6,98	0,8			
			7,16	0,84			
			6,33	0,86			
	Pöytäkone ethernet-liitynnällä		7,1	0,88			
			7,05	0,88			
			7,07	0,88			
Koe 6							
Lähettävä WLAN tukiasema	A-link RR24AP ADSL 2/2+ modem	Channel 1	Verkossa 4 päätelaitetta WLAN:n välityksellä. Kaksi suoraan A				
ei salausta	b/g						
	AP						
Repeater	Zyxel WRE2205						
	HP Elitebook 8560p	AP/WDS	7,06	0,91			
			7,08	0,91			
			7,06	0,91			
		ilman toistinta	7	0,9			
			7,06	0,91			
			7,07	0,91			